제1주제

한국에서의 국민식별번호와 인터넷 본인확인

한국에서의 국민식별번호와 인터넷본인확인[1)]

한 상 희*

목 차

Ⅰ. 서론

정보화가 사회구조의 변화에 어떠한 영향을 미치고 있는가는 보는 관점에 따라 다를 수가 있다. 더욱이 그것이 미래에 어떠한 결과를 야기할 것인가에 대하여는 더욱 다양한 논의가 제시될 수 있다.[2)] 하지만, 적어도 현상으로서 또는 예측가능한 변화수준이라는 점에서 정보화의 사회구조적 영향을 서술할 수는 있을 것이다. 왜냐하면 정보화는 미래학자들이 주장하듯 자유와 자기지배, 자기실현의 기회가 넘치는 찬란한 미래를 약속하고 있기도 하지만, 그와 동시에 기술회의자들이 말하듯, 기존의 권력관계가 그대로 관철되거나 강화되는 계기로서 작용하기도 한다. 그것은, 그 동안 소수의 정치적·경제적 권력엘리트의 수중에 장악되어 있던 정보에 일반인들이 접근할 수 있는 통로를 제공하는 한편, 그것은 그 정보네트워크를 따라서 기존의 권력집단들이 자신들의 권력을 강화할 수 있는 가장 효율적이고 능동적인 메카니즘을 구축할 수 있도록 한다. 그리고 이를 통하여 개인의 일상생활을 항시적으로 감시·감독할 수 있는 터전을 제공한다. 또는 정치경제학적 수준에서 본다면, 경제적 이윤추구의 동기에 굴복하여 삶의 폭을 획일화하고 편협한 것으로 만들어 버

* 건국대 법학전문대학원 교수

1) 이 글은 프라이버시 워킹 그룹의 도움을 바탕으로 쓰여졌다. 특히 본인확인제에 관련한 실태조사나 문제점의 적시 등은 이 그룹에서 작성한 것을 원용하였다. 특히 장여경, 윤철한, 전응휘 선생님의 도움은 절대적이었다. 물론 이 글의 내용은 전적으로 발제자의 책임에 속한다.

2) 이는, 세 가지 정도의 입장들-신미래학자(neofuturists), 기술회의론자(teletechnology dystopians), 그리고 기술현실주의자(technorealists)-로 정리될 수 있다. A. G. Wilhelm, Democracy in the Digital Age(New York: Routledge, 2000), pp.14-23

릴 가능성 또한 없지 않다.

이 글은 이렇게 개인을 향하여 전방위적으로 투사되고 있는 감시의 눈길을 다루고자 한다. 벤담이 창안하고, 조지 오웰의 소설 「1984년」에서 가상적인 형태로나마 실천되었고, 푸코가 그토록 경계하였던 판옵티콘, 그 원형감옥은 오늘날 더 이상 국가의 전유물이 아니다. 밀레니움의 전환기를 거치면서 급속도로 발전하는 기술은 항시적, 전방위적, 그리고 편재적 감시체제를 국가의 손으로부터 약간의 비용부담의 의지가 있기만 하다면 그 어떤 자의 손에도 쥐어줄 수 있도록 하였다. 전사회적인 수준으로 감시 '권력'이 확산되는 현상을 초래하고 있는 것이다. 그래서 R. Whitaker가 말하는 「감시국가에서부터 감시사회로」의 전이가 의미를 가지게 된다.[3] 그는 감시사회를 말하면서 주로 기업에 의한 소비자 감시 즉, 고객서비스라는 이름으로 주어지는 각종의 혜택을 미끼로 소비자정보를 수집하고 이를 바탕으로 혜택을 받을 자를 선별하면서 위험인물이나 (소비자로서의) 자격미달자를 배제시키는 데이터감시를 중심을 설명한다. 그가 말하는 참여적 판옵티콘(participatory panopticon)-피감시자의 자발적 혹은 추정적 동의에 의한 감시체제-는 이를 지칭하면서, 기업이 이윤추구의 목적을 위하여 일종의 마케팅전략의 일환으로 전방위적 감시의 망을 구축하는 가운데, 사람들은 시민(citizen)이 아니라 소비자(consumer)로 전락하게 됨을 비판하고 있다.

대체로 감시체제는 그 영역에 따라 국가감시, 작업장감시, 소비자 감시 등으로 나뉠 수 있으며 그 감시의 양태에 따라 쌍방향적 감시와 일방향적 감시로 구분할 수 있다. 대체로 국가감시와 작업장감시는 소비자 감시와 다른 맥락에서 거론된다. 국가감시나 작업장감시는 법률이나 고용계약과 같은 포괄적 지배체제하에서 국가 또는 사용자/관리자가 일방적으로 국민이나 노동자의 신원이나 신분관계, 거주관계 혹은 그의 행동이나 성과, 성품 등을 감시하고 이에 대해 국민이나 노동자는 복종할 것이 의무 지워지는 일방향성으로 특징 지워진다. 반면 소비자 감시는 새로운 유형의 감시사회에 해당되는 감시유형으로 적어도 외관상 참여적 판옵티콘의 체제를 이룬다. 즉, 소비자들은 판매자의 유혹에 대한 동의의 형식을 통해 자신에 대한 감시를 자발적으로 수용하면서 그 댓가로 일정한 혜택을 수령하는 구조를 띤다. 개인이 자신의 정보를 제공하고 정보수령자는 그에 대해 마일리지라든가 포상과 같은 대가를 교환하는 순수한 사적 거래의 형식을 취하는 것이다.

그러나 소비자감시의 메카니즘은 이런 순수형에 머무르지 않는다. 단일 상품에 대한 단일 거래의 경우에는 이런 순수형의 사적 거래로서 종결될 것이지만, 계속적으로 이루어지는 거래관계라든가 혹은 복수의 거래가 포괄적·연쇄적으로 일어나는 경우 또는 독·과점적 지위에서 이루어지는 경우에는 전혀 다른 모습이 된다. 모든 상품과 모든 서비스가 다 집약되어 있는 인터넷 쇼핑몰이나 모든 정보가 집적되어 있는 포털과 같은 경우가 이에 해당한다. 단순간에 완료되는 거래가 아니라 앞으로도 계속하여 거래가 이루어질 것이고, 또 그 곳을 통하지 않으면 사실상 거래가 불

3) 이에 관하여는 R. Whitaker, The End of Privacy(Melbourne: Scribe Publications, 2000) 참조.

가능하거나 혹은 고비용의 한계에 빠지게 되는 위험까지 안고 있는 경우이다. 이런 상황에서는 소비자 감시의 문제는 국가감시나 작업장감시와 마찬가지로 일방향적으로 이루어진다. 개인정보를 제공하는 댓가로 받는 편익이 결코 무시할 수 없는 수준에 이르고 있는 만큼 일반적인 소비자들이 그 개인정보의 제공 혹은 감시에의 종속을 거부할 수 없는 사실상의 강제가 작용하는 것이다. 혹은 휴대폰과 같은 생활필수적인 서비스의 경우에는 그 부의 편익이 가지는 불편함이 이런 사실상의 강제를 야기한다.

문제는 여기에서 나온다. 그 감시의 구조와 효과-후술한다-는 국가감시와 거의 동일함에도 불구하고 그 감시의 관계가 설정되는 계기와 영역에 있어서는 전통적으로 별개의 개념화작업을 통하여 논의되고 있다. 국가감시의 경우에는 소위 「공적 영역」이라는 관념 속에서 국가권력으로부터의 자유라고 하는 고래의 인권관념과 더불어 정치과정·통치과정의 민주화의 요청이 적용되고 있는 반면, 작업장 감시나 소비자 감시의 경우에는 첫째, 감시의 전제가 되는 계약 자체가 「사적 영역」으로 획정되면서 그것이 쌍방간의 합의에 의하여 형성되는 것으로 간주되고 있다는 점에서, 그리고 둘째, 재산권의 비인격화현상과 대응하여 노동자 및 소비자의 인권 또한 하나의 상품 내지는 재산권으로서 이전의 대상이 되는 동시에 그에 대한 지배권이 사용자에게 이전되는 형식으로 개념화되고 있다는 점에서 문제가 발생하게 된다. 국민국가와 국민의 관계에서 통상적으로 실시되는 감시는 그 자체 권력성이 인정되면서 「공법적」 규제의 대상이 되는 반면, 사용자의 노동자에 대한 감시와 판매자의 소비자에 대한 감시는 고용관계 내지는 임노동관계에 선행하는 고용계약과 그 전제로서의 사적 재산의 절대라는 관념에 의거하여 「사법적」 규율의 대상에 머무를 뿐, 그로 인하여 발생하는 노동자의 프라이버시의 권리에 대한 제한 내지는 프라이버시의 물화·상품화현상에 대하여는 전혀 속수무책인 것이다.

이 글은 이러한 문제점을 중심으로 작업장에서 일어나는 각종의 감시체제에 대한 (헌)법적 이해를 모색하고, 이를 바탕으로 우리나라에서 현재 시행되고 있는 본인확인제도의 현황과 그 문제점을 살펴보고자 한다. 이를 위해 우선 제2장에서는 개인식별번호제를 기반으로 이루어지는 국가감시를 비롯한 감시 일반의 문제점을 검토하고 제3장에서는 본인확인제에 대한 헌법재판소의 판단을 정리한 다음, 이어서 “사적” 영역에서 이루어지는 본인확인제의 실태와 그 문제점, 그리고 그 개선방안을 검토해 보기로 한다.

Ⅱ. 국가감시와 국민식별번호

1. 국가감시의 정치학

국가감시(state surveillance)는 감시사회의 기본틀을 이룬다. 그것은 Giddens의 말[4]처럼 관료제 체제를 특징으로 하는 근대국가에서 필연적으로 드러나는 현상 중의 하나로 국가가 행정의 효율성을 향상시키거나 복지서비스를 실효성 있게 제공하는 가장 유효한 수단중의 하나로 국민감시의 체제를 확보하고 또 가동한다. 치자인 국가가 피치자인 국민에 대한 정보를 수집하고 관리함으로써 기본적인 행정영역을 구축하고 이를 바탕으로 국가와 국민의 관계들을 설정, 관리, 집행하는 것이다. 그리고 이러한 현상은 오늘날과 같은 행정국가적 현상이 가중되는 국가체제라든가 냉전적 국가관리체제 혹은 대테러목적 등의 국가·사회안보에 중점을 두는 국가체제에서는 더욱 강화될 뿐 아니라 그 감시의 강도나 심도 또한 더욱 고도화되는 추세를 보이기도 한다.

하지만, 문제는 이러한 국가감시가 또 다른 면도 가지고 있다는 점이다. 그것은 안보와 질서, 행정의 효율성이라는 점에서는 正의 기능을 수행하기도 하지만, 역으로 감시의 대상인 국민들에 대한 사생활의 침해와 그에 기반한 강력한 권력현상을 야기한다. 나아가 이 일방향적 권력현상에 의해 민주주의의 기본틀까지도 왜곡될 위험을 야기하기도 한다. 나치정권이나 구동독, 혹은 Stalin체제하에서의 소련의 경우처럼 전체주의적 국민관리의 수단 혹은 국가내부의 위험인자(안보위험인자 혹은 질서위험인자)를 적발하고 처리하기 위한 수단으로 기능하기도 하는 것이다.

이런 체제하에서는 국민의 지위 자체가 심각하게 교란되어 버리고 만다. 국가과정을 능동적으로 구성해 나가는 참여적 시민이 아니라, 국가가 원하는 모습으로 가공되고 변형된 시민 혹은 국가과정으로부터 교묘하게 배제되고 소외된 시민들이 속출하는 상황이 벌어지게 되는 것이다. 이 점은 국가감시의 가장 기본적인 형태인 모니터링에서 잘 드러난다. 이것은 불특정 다수의 시민을 상대로 그들의 구체적인 행동이나 신원을 포착하고 일정한 기준에 해당하는 행동 또는 신원자를 식별해내기 위한 포괄적이고 무차별적인 감시활동으로 이루어진다. 그리고 그것은 세 가지의 목적에 봉사한다. 첫째 모니터링은 국민에 대한 다양한 정보를 제공한다. 국가가 원하는 정보설계에 따라 필요한 정보요소들을 추출하는 것이다(정보수집으로서의 모니터). 둘째 그것은 모니터의 대상이 되는 감시대상자들을 다른 일반인으로부터 구

4) A. Giddens, 진덕규 역, 민족국가와 폭력, 삼지원, 1991, 2130215면 참조. Giddens에 의하면 공동체 중심사회를 국민국가(nation state)가 대체하면서, 근대국가는 그 재정적 수요와 더불어 상설적인 군사력을 관리하기 위하여 국가내의 모든 자원들에 대한 관리체제를 구축하여야 한다. 나아가 국가는 인력이나 재정 등 자원의 확보 및 집행을 위한 '분배적 자원'(계획이나 행정)과 법집행 및 경찰작용을 관철시키기 위한 '권위적 자원'(권력과 통제)의 양자를 확보하여야 하며 '정보사회'는 이 점에서 필연적으로 나타나기 마련이다. 요컨대, Giddens의 국민국가는, 정보를 항시적으로 추구하는, 감시를 필수적인 기초로 삼아 운영되는 국가-감시국가(surveillance state)일 수밖에 없는 것이다.

분하고 구획하기 위한 작업이다. 국가가 설정하는 일정한 기준에 따라 국민들을 구획하고 이 구획선의 어느 한 쪽에 있는 자에 대하여 처벌이나 배제, 사전검속 등과 같은 소극적 제재를 가하거나 혹은 그들을 추적할 수 있는 기회를 확보하기 위하여 이루어지는 작업인 것이다(위험배제 또는 지배로서의 모니터).

셋째, 하지만 이 모든 것보다 더 문제적인 것은 이 모니터링을 통해 이루어지는 훈육이다. Faucault의 판옵티콘이 수행하는 주된 기능이 여기에 해당한다. 감시자 또는 모니터를 하는 자는 전체 사회나 전체 대중에 대하여 그러한 감시 또는 모니터가 이루어지고 있음을 주지시키고 그에 의하여 일정한 공적 제재가 가해짐을 알림으로써 피지배자인 대중들이 그러한 규율 자체를 자신의 의식 속에 내재화하도록 유도하는 일종의 지배의 수단으로서의 기능을 말한다(훈육으로서의 모니터).[5] 그래서 사회적 관계들을 분할하고 계열화, 위계화함으로써 권력현상이 사회 모든 부분에 편재하도록 만들고 이런 사회구조를 사회의식의 수준에서 정당화하고 그것을 정상적인 것으로 인식하도록 대중의 의식 자체를 바꾸어버리는 것이다. 그리고 감시국가에서의 국가주의는 이렇게 완성된다.

넷째, 모니터링으로 획득된 다양한 개인정보들을 연동을 통해서 새로운 시민-일종의 가상적 시민(virtual citizen)-들을 양산하게 한다. 여러가지의 정보들을 서로 결합시키거나 혹은 그 정보(들)에 일정한 알고리즘을 적용, 당해 정보주체에 대하여 어떠한 가치판단을 내릴 수 있는 제2차·제3차 정보를 생산하게 만드는 경우 그 폐해는 이루 말할 수 없게 커진다. 예컨대, 컴퓨터가 인공지능을 갖추고 자기성찰적(self-reflexive) 기능을 수행하면서 어떠한 판단을 내리고 이에 기하여 그 다음의 절차를 진행하는 자동화의 상황은 한 예가 된다.[6] 혹은 반의 국가과정에 적극적으로 참여하는 능동적 시민으로서의 국민이 아니라, 국가는 자신이 수집, 관리하는 정보에 의하여 국가가 요구하는 틀에 맞는 일정한 프로파일을 만들고 이에 따라 그 국가작용의 내용과 형식, 절차를 결정하는 과정은 또 다른 예가 된다. 사회 내에는 현실의 시민이 아닌 가상적 시민만이 존재하고 되고 여기서 파생되는 시민의 소외현상은 민주주의의 가장 본질적인 내용까지 침해하게 되는 극단적 상황까지도 예견할 수 있게 하는 것이다. 바로 이 점에서 국가감시의 문제를 단순히 개인정보에 대한 자기통제·관리권의 맥락에서만 파악하고 있는 우리 (헌)법학계의 입장은 문제를 안고 있다. 국가감시의 문제는 개인적 기본권의 문제이자 동시에 민주주의 그 자체의 문제인 것이다.[7]

이는 특히 다음과 같은 형태로 발현된다.

---

5) 후술하듯 주민증이 국민 혹은 양민(良民)으로서의 아이덴티티를 확인하는 증표로 이용되는 것은 이를 단적으로 드러낸다. 스스로 "빨갱이"가 아님을 증명하도록 함으로써 그 "빨갱이"를 사회적 터부로 만들어버리는 것이다.

6) 키보드 입력시간 통제, POS(Points of Sales) 시스템 등과 같은 작업장감시의 자동경보메커니즘에서 사용되는 다양한 시스템들은 그 두드러진 예가 된다. 자세한 것은 고영삼, 전자감시사회와 프라이버시, 한울아카데미, 1998, 179-202면 참조.

7) 이런 논의는 "훈육에서 스마트 통치로" 이행하는 과정을 서술한 이광석, 지배양식의 국면 변화와 빅데이터 감시의 형성," 사이버커뮤니케이션 학보, 제30권 제2호, 2013, 191-231면, 특히 199-202면 참조.

1.1. 국가/시민사회/개인의 단절: 그것은 국가와 국민생활의 괴리현상을 야기하여 자의적인 국가작용이 이루어질 수 있게 한다. 정보화의 과정에서 국가가 수집하는 정보들이 현실생활과는 다른, 기호화·분편화된 형태의 단위정보로 구성되고 그것이 다시 국가에 의하여 형성되는 체계에 의하여 재조합되는 과정에서 국민들의 욕구와 의지들이 국가 자체의 욕구와 의지에 의하여 획일적으로 구성되는 왜곡된 현실을 야기할 수 있다.[8] 국가가 수집한 단편적인 정보들이 그 자체의 수행성원리에 의하여 역으로 국민생활을 엮어내고, 국가는 이렇게 인공적으로 조합된 가상적 생활을 실제의 국민생활로 파악하게 되는 단절적 상황이 발생할 수 있는 것이다.[9] 역으로 국민들은 자신의 생활상의 욕구를 제대로 국가에 반영시킬 수 있는 기회를 박탈당하게 된다. 한마디로 국민들은 경직된 국가정보활동에 의하여 자신을 대표(representation)할 수 있는 기회를 제한당하는 것이다. 그래서 국민에 의한 정부가 아니라, 정보에 의한 정부라는 민주적 정치과정 자체가 위협받게 되는 탈정치화의 상황이 벌어질 수도 있다.

1.2. 관료주의·행정편의주의에 따른 생활세계의 왜곡가능성: 이러한 단편적 정보에 대해 관료적 합리주의 내지는 관료주의적 편의주의가 작용하게 되는 경우에는 그 나마의 정보마저도 취사선택되거나 왜곡됨으로써 국민생활은 더욱 더 국가작용으로부터 소외되고 그 반작용으로 국가는 전례 없이 강력한 권력을 장악하거나 자의적인 권력행사를 초래하는 등의 역작용이 예상될 수 있다. 전문적 지식을 갖추고 있는 행정관료들은 일반국민에 비하여 엄청난 양의 정보들을 자신의 패러다임에 상응하게 분석하고 처리할 수 있음으로 인하여 정보시스템의 쌍방향성의 특성조차도 부인하고 독단적이고 자의적인 결정으로 나아갈 수도 있다. 또한 정보의 쌍방향성은 행정업무의 저효율성을 초래하거나 역으로 행정관료의 독단을 정당화하는 기능을 할 가능성도 있다. 수많은 민원사항이 정보망을 통하여 동시다발적으로 제기됨으로써 한정된 자원을 가진 정부로서는 대처불능의 상황에 빠질 수도 있고 또 그를 이유로 행정관료가 이 정보들을 자의적으로 선별하여 부분이익만 정책으로 반영하는 행태를 야기할 수도 있는 것이다.

1.3. 초감시국가 – 절대권력의 가능성: 국가는 경우에 따라 국민들 간의 의사소통과정을 감시하고 통제함으로써 국민들의 생활관계 내지는 생활양식 자체에 영향을 미칠 수도 있다. 정보통신기술의 발전이 냉전체제와 복지국가의 요청에 의하여 이미 강화된 정보국가로 하여금 보다 효율적인 형태로 국민들을 항시적으로 감시하고 통제할 수 있는 틀을

8) 실제 2004년의 한 언론보도에 의하면 당시 호적정보시스템에 등록된 5,200여만 명 가운데 10%가 넘는 550만 명의 주민등록번호가 잘못 기록되어 있는 것으로 조사됐다(MBC 9시 뉴스데스크, 2004년 7월 7일자): 장종인, "개인정보시장에서 주민등록번호의 이용," 정보통신정책 제17권 제18호, 2005, 28면. 이런 오류는 그 자체 국가작용으로부터 그 당사자들이 배제될 수도 있는 위험을 야기하게 된다. 또한 주민등록 자체가 말소되는 경우에는 엄청난 불이익을 안게 된다. 이에 대하여 자세한 것은 국가인권위, 주민등록말소자 기초생활 실태조사: 2006, 국가인권위원회, 2006 참조.

9) 국민기초생활보장법상의 부양의무제는 이러한 단절의 대표적인 예가 된다. 자세한 것은 전국장애인차별철폐연대, 상반기 전국 순회자료집, 전국장애인차별연대, 2013, 24-31면 참조.

확보할 수 있도록 하고 있기 때문이다. 하지만 문제는 국가를 중심으로 모든 국민생활들이 중앙집권적인 통제 하에 놓이게 되는 상황에만 한정되지 않는다. 그것은 국가가 관리하는 정보를 중심으로 국민들이 자신들의 생활을 재구성하도록 한다는 점에서 더욱 더 악화된다.[10] 국가가 자신에 관한 정보를 확보하고 있고, 그것을 통하여 자신의 일상생활을 포착하고자 노력하고 있다는 인식으로 인하여 개개인들이 자신의 일상생활을 스스로 통제하게 되는 현상이 보편화될 소지가 있는 것이다.

2. 주민등록제와 초감시국가

요컨대 오늘날 가장 중요한 헌법문제는 이 초국가로서의 감시국가이다. 그것은 국민을 주권자로 만들기 보다는 스스로를 국가의 대리인으로 상정하는 관료들로 하여금 주권적 권력을 작동할 수 있는 여지를 마련한다. 소수에 의한 다수의 통제가 이루어지며 사생활과 사적 결정권을 중심으로 하는 인권과 인격의 본질적 침해가 이루어질 위험을 안고 있기 때문이다.

실제, 국민들은 일종의 자기검열에 의하여 국가가 원하지 않는 행동을 자발적으로 회피하는 동시에 그러한 생활방식 자체를 자신의 것으로 내재화함으로써 스스로를 국가에 길들이는, 그럼으로써 자신을 국가에 종속시키게 되는 전방향적 통제국가가 등장하게 된다. 비유적으로 말하자면, 모든 국민의 생활을 자신의 감시와 통제하에 두고 있는 조지 오웰의 Big Brother와 같은 국가의 수준을 넘어서, 그 감시에 길들여진 국민들은 미리 국가의 의사에 자신의 생활을 순응시키게 되는 Foucault식의 Panopticon이 등장하여 국가의 실체를 이루게 되는 셈이다.

주민등록제도는 이러한 자기검열과 자기순치의 훈육효과를 극대화하는 매개가 된다. 개인에 관한 주요한 정보를 자신의 거주지와 동거가족을 중심으로 수집 당하고 주민등록번호라는 생애불변의 고유인식자를 바탕으로 자신의 모든 생활정보를 드러내어야 하는 상황에서는 언제나 자신의 행동에 대한 자기검열은 불가피하게 된다. 언제 어디서라도 들여다 보여질 수 있다는 인식, 그리고 그러한 감시가 자신도 모르는 사이에 이루어진다는 무지의 베일이 양자가 판옵티콘의 절대권력을 형성한다는 것은 벤담만의 지혜는 아닌 것이다.

그리고 이 점에서 그것은 민주주의와 법치주의를 침해한다. 초감시국가가 야기하는 세 가지의 문제 - 국가와 시민사회의 절대적 분열 및 시민사회의 탈정치화, 관료중심의 국가행정체제, 그리고 시민사회 및 개인의 생활에 대한 국가의 가부장적 후견과 개입 - 은 이미 권위주의적 국가주의의 가장 두드러진 특징으로 등장한다.[11] 첩보로부터 정보를 골라내고, 이를 자신이 정립한 목적을 위하여 체계화하고

10) 한겨레신문의 보도에 의하면 심모라는 사람은 출생당시 주민등록번호의 앞자리만을 부여받았기 때문에 주민등록을 제대로 하지 못 한 채 46년을 살면서 고등학교 진학도 하지 못 하였고, 내내 실업상태로 오대산에서 야영생활을 하며 20여 년을 살았다고 한다. 주민등록이 없다보니 학교진학을 거부당하고 간첩의혹, 불심검문 등의 어려움을 겪어야 했다고 한다. 2005년 3월에 민변의 도움으로 주민등록증을 발급받았다고 한다(한겨레신문, 2005년 5월 25일자). 장종인, 앞의 글, 29면에서 재인용.

11) 우리나라의 권위주의적 헌법현실에 관한 분석으로는 한상희, 앞의 글 참조.

그 목적의 달성에 필요한 형태로 가공하고 처리해 내는 작업들 모두가 바로 이런 국가주의의 전형적인 모습인 것이다. 그리고 이러한 초국가(superstate)로서의 감시국가(state of surveillance)는 "정보관료제"[12]는 엄청난 부가가치를 지니는 무한의 정보를 확보하면서 그 정보불균형을 토대로 또 다른 권력을 행사할 수 있게 된다. 감시활동을 통한 경찰력의 강화뿐 아니라 도덕적 전체주의, 정보화구국론, 대테러적 가치의 선전, 국가정보기구의 팽창, 지도자에 대한 개인숭배와 같은 직접적 권력뿐 아니라 정치적 무관심의 조장이라든가 정치적 데마고그의 동원 등 다양한 방식으로 권력의 집중과 전횡의 가능하게끔 할 수 있게 되는 것이다. 이하에서는 이러한 전방위적 감시의 틀로 구성되어 있는 주민등록제-특히 주민등록번호제를 살펴보기로 하자.

2.1. 국민등록제와 주민등록제[13]

대체로 국가가 국민을 관리하는 체계는 국가신분제 내지는 국가신분증명제로 대변된다. 개개인의 신분은 그 사람의 지위와 권리를 특정하는 가장 기초적인 지표가 된다는 점에서, 그리고 이러한 지표를 바탕으로 국가는 그에 대한 징집이나 과세 기타 공적 규제와 관리를 할 수 있게 된다는 점에서 국가신분제는 근대국가의 기본요소를 이룬다. 이는 국가나 지방자치단체가 국민(경우에 따라서는 외국인도 포함됨) 혹은 주민의 신분을 확인하고 이를 공부(公簿)에 등록하는 방식으로 이루어진다. 호적제도나 가족부제도는 그 예로서, 전자는 이 신분을 가(家)를 중심으로 법률로 정한 가(家)의 범위에 따라 편제하는 가(家)별 편제방식이며, 후자는 개인 혹은 그의 가족을 중심으로 편제하는 개인별/가족별 편제방식이다. 그 외에도 한 사람의 인격이 아닌, 그 사람의 일생사를 중심으로 하는 사건별 편제방식도 있다. 즉, 독일이나 미국, 프랑스의 경우처럼 그 사람의 출생, 사망, 혼인 등 사건별로만 편제하고 이를 따로 개인별로는 편제하지 않는 경우가 그것이다.[14]

반면, 주민등록제는 일정한 지역공동체나 생활공동체를 바탕으로 그 구성원들을 파악, 관리하기 위한 일종의 행정적 목적을 위한 것이다. 즉, 그것은 지역공동체나 생활공동체에 정주(定住)하는 사람들을 일정한 행정관청에 등록하게 함으로써 정주민-주민-의 거주관계나 상시 인구동태를 파악하고 이를 각종 행정의 기반으로 삼거

12) 고영삼, 앞의 책, 293면, 또한 285면도 참조.

13) 이하의 서술은 이은우, 「신분등록 및 주민등록제도의 개선방안」, 건국대학교 법학연구소, 『국가신분등록제와 프라이버시권의 충돌과 대안』, 학술토론회 자료집, 2003. 10. 31을 주로 참고하였음

14) 여기서 우리나라와 같은 방식의 국가신분등록제도는 한 사람의 권리의무관계를 명확히 한다는 점에서는 나름 강점을 가진다고 할 수 있으나, 하나의 공부에 지나치게 많은 개인정보들을 담아냄으로써 그의 혈연관계나 신분관계를 손쉽게 추적해 낼 수 있다는 단점을 가진다. 특히 종전의 호적방식은 중국의 경우처럼 단순한 가족만을 등록하는 것이 아니라 확장된 혈연개념인 가(家)와 그 가의 소재지(본적지)를 바탕으로 등록하게 만듬으로써 생계여부와 혈연여부 및 그 지역적 생활관계를 동시에 등록하게 만들기도 하였다. 이 호적방식은 성별에 의한 차별금지라는 헌법명령에 의하여 위헌판단을 받음으로써 이제 가족부방식으로 바뀌기는 하였지만, 현행의 가족부방식 역시 너무 많은 정보를 하나의 공부에 담아내고자 한다는 점에서는 크게 나아진 제도라 하기는 어렵다고 할 수 있다.

나 혹은 그 행정의 목적으로 하고자 하는 제도다. 따라서 앞서 언급한 국민등록제도와는 달리 이 주민등록제는 그 행정목적이나 행정방식에 따라 도입하는 경우도 있고 그렇지 않는 경우도 있으며, 전자의 경우에도 국가가 관리하는 경우와 지방자치단체 등이 관리하는 경우로 나뉘기도 한다. 예컨대, 미국, 아일랜드, 오스트레일리아, 캐나다 등과 같은 나라들은 주민등록제도-전국민을 대상으로 주민등록을 하게 만드는 제도-를 두지 않고 개별적인 사안/사건별로 등록할 필요가 있는 경우에만 등록하게 하는 나라들이다. 예컨대 영국의 경우에는 납세관리(주로 Council Tax)의 목적으로 주민등록을 하게 하며, 미국의 경우에는 선거인등록이 대표적이다. 엄밀히 보자면 강제적인 국민(주민)등록제도를 두고 있는 나라들은 소수이다.

2.2. 주민등록제도와 그 문제점

그러나 우리나라의 신분/주민 등록제도는 무엇보다 양자가 서로 중복되어 있을 뿐 아니라 불필요하게 많은 정보들을 담고 있다는 점에 그 문제점이 있다. 뿐만 아니라 이 모든 정보들이 강제적으로 제출 혹은 수집되도록 하고 이를 거대한 국가 데이터베이스에 통합, 관리할 수 있도록 한다는 점도 문제다. 그 중에서도 주민등록제도는 주민등록번호라는 통일적, 불가변적 식별자를 사용하여 모든 국민을 일생 전반에 걸쳐 통합관리할 수 있도록 하고 있음은 가장 큰 문제를 이룬다. 국가가 시민사회를 통치의 대상으로만 규정하고 그 위에 군림할 수 있는 강력한 정보권력을 부여하고 있는 것이다.

2.2.1. 국가신분등록제의 연혁[15]

우리나라에서의 주민등록제도는 저 멀리 일제강점기로까지 소급된다. 일제는 식민지조선의 주민들을 관리하고 인적·물적 자원들을 수탈하기 위한 수단으로 1909년의 민적법(民籍法)과 1922년의 조선호적령(朝鮮戶籍令) 등을 통해 조선의 전통적인 호적제도를 없애고 일본식의 가(家)를 중심으로 하는 신분등록제를 확립하였다. 일제는 호주(戶主)를 만들고 이 호주를 중심으로 남계혈통에 해당하는 가족들을 가(家)라는 관념적 집합체에 편입시켜 이를 대대로 영속시키면서 그 기본적인 승계체제를 직계비속남자에 연결시키는 신분등록방식을 취하였다.[16] 즉, 모든 사람을 국가신분체제에 편입시키면서 가(家)의 중심이 되는 호주와의 관계를 기준으로 그 사람의 신분됨을 획정하였던 것이다.[17]

문제는 이러한 신분제도는 토지와 인간이 밀접히 연결되어 있는 농경사회에서는 본적을 중심으로 그 사람의 법률적 관계를 증명하는 데는 큰 도움이 되었을 것[18]이

---

15) 이 부분 서술은 주로 김영미, “해방 이후 주민등록제도의 변천과 그 성격 - 한국 주민등록증의 역사적 연원-,” 한국사연구, 제136호, 2007, 287-323면을 참조하였음

16) 헌법재판소, 2005. 2. 3. 선고 2004헌가5 민법 제778조 위헌제청

17) 김병유, “주민등록제도의 의의와 연혁 개관,” 사법행정, 1979. 12. 103-104면

18) 실제 일제의 호적령 자체가 혈연을 기반으로 하는 것이기 보다는 그 혈연집단의 거주지, 즉 ‘본적지’를 중심으로 구성되어 있다는 점에서 그 기본적 지향은 신분관리와 더불어 정착농업에 기반한 봉건사회

나 이러한 농경사회 혹은 지역공동체적 생활방식이 해체되는 상황에서는 그 사람의 현재 상태를 파악하고 감시하기에는 별다른 기능을 하지 못 하였다. 그의 호적지-즉 본적-와 거주지가 다른 경우에는 속수무책이었던 것이다. 특히 일제하에서 진행되었던 도시화와 이향민(離鄕民)의 증가현상은 자원동원이 절실하였던 군국주의체제 내지는 전시체제에서는 더더욱 행정불편을 야기하게 되었다. 이에 일제는 1942년 조선기류령을 선포하여 주거지 신고의무제를 실시하였다. 90일 이상 본적지를 떠나 거주하는 자, 또는 본적이 불분명한 자는 이 사실을 거주지 관할 행정기관에 신고해야 하며, 관할 행정기관은 이 정보를 본적지에 연락하여 호적에 기록하도록 하였다. 그리고 이러한 신분등록제를 통해 1944년의 징병제를 비롯한 다양한 전시인력동원 및 물자동원을 효과적으로 수행할 수 있었다.

해방이 된 연후에는 미군정이 이 기류령을 반복한다. 미군정은 1947년 1월 '인구 동태의 정확성'과 '투표' 등의 목적으로 전 국민이 거주등록을 하고 '등록표'를 발급받을 것을 요구하였다. 이는 북한에서 1946년 9월부터 실시하던 공민증에 갈음하는 것으로 '남조선의 합법적 주민인 것을 증명'하는 용도로 홍보되었다고 한다.[19] 이 등록표에는 등록번호가 기재되었으나 그것은 지역의 고유번호와 등록순서를 기재한 것으로 추정되고 있다. 이 등록표는 항시적인 소지의무가 부여되어 국가검열, 통제의 수단으로 이용되기도 하였다. 등록표에 하던 지문날인에 대하여 당시 민정장관이던 안재홍이 "등록표에 지문을 받는 것은 현재의 사태가 과도기에 있는 만큼 경찰 수사상에도 필요함으로 그리한 것이다"(동아일보, 1947. 3. 20)라고 발언한 기록이 있는 것을 보면 좌익세력 색출을 중심으로 한 경찰목적의 수단으로 이용된 것이라 보아 잘못됨이 없는 것이다.

1949년 '빨치산 토벌지역'에서 발급된 "국민증"은 이런 치안적 성격을 명확히 한다. 그 국민증의 관할청은 경찰청으로 일정한 시간간격(6개월?)을 두고 경찰청의 검인을 받도록 하였다. 그중 경북지역에서 발급된 국민증에는 우무인과 좌무인을 날인하고 이에 경찰서장의 검인이 첨부되어 있다. 즉, 경찰이 주관하여 "공비"와 "주민"을 구분하는 증표로써 이 국민증을 사용한 것이다. 그리고 한국전쟁 중에는 이런 국민증이 전국에 걸쳐 확대 시행되었고 거기에도 여전히 우무인·좌무인의 날인이 행해졌다. 이 국민증은 14세 이상의 모든 남녀가 보증인 2명, 반장, 통장, 동회, 경찰서의 5단계 심의를 거쳐 발급받도록 하였다. 다만, 이때의 국민증은 지방자치단체 단위로 발부되어 시민증 내지는 도민증의 형식을 취하였다. 하지만, 그 형식의 차이에도 불구하고 이 시민증·도민증은 주기적인 갱신절차와 함께 경찰의 불심검문의 주된 목표가 되었다. 즉, 항시적 소지·제출의 의무를 부과하고 이를 바탕으로 '양민'과 '간첩'을 구분하는 수단으로 이용되었던 것이다.[20]

에서의 거주민관리에 있었다고도 할 수 있다.

19) 여기에는 ①시일(등록번호), ②성명, ③연령, ④신중(몸무게), ⑤신장, ⑥신체 특징, ⑦직업, ⑧고용주, ⑨서명(지문), ⑩발행자(면장), ⑪발행자의 서명 등이 기재되어 있었다고 한다.

20) 1959년 9월 3일 다가오는 대통령선거의 전략을 발표하는 와중에 자유당 당무회의에서는 시·도민증의 폐지는 시기상조라고 하면서 그 이유를 다음과 같은 7가지를 내세웠다. ①간첩색출에 절대 필요하다, ②불심검문의 계기가 된다, ③간첩기소의 증거물이 된다, ④간첩이 위조하더라도 경찰을 그것을 적발할 수

이러한 시・도민증 제도는 4.19혁명과 함께 유명무실화되다가 5.16 쿠데타 이후에 다시 부활한다. 쿠데타세력이 반공을 내세우자 시민들은 “자신의 안전을 보장할 첫 번째의 조치로서 시민증부터 발급받았던 것이다.” 그리고 이런 흐름 속에서 1942년의 조선기류령을 확대 강화한 1962. 5. 10. 주민등록법이 제정, 공포된다.

이 주민등록제도는 일제의 기류법의 전통과 해방 이후의 국민증 체제를 복합하여 확립된다. 그것은 다른 나라에서 흔히 보듯 사회복지혜택이나 국가적인 서비스의 제공을 위한 신분관리체제를 구축하려는 목적이 아니라, “간첩이나 불순분자를 용이하게 색출·식별하는 등, 모든 국민을 효과적으로 관리하려는 목적으로 도입되었다.”[21] 실제 1968년 1.21 청와대기습사건과 1.23 푸에블루호사건을 계기로 시・도민증을 폐지하고 주민등록번호가 기재된 주민등록증을 발급하는 주민등록법의 개정이 이루어질 당시 내무부의 언론홍보는 이 점을 분명히 한다.

새로운 개정안이 통과되면 주민등록은 호적과 일치되게 내용을 일일이 본적지에 조회하여 통일하게 되므로 국민들의 주거실태를 정확히 파악할 수 있다는 점에서 시・도민증보다 북괴간첩의 잠입을 막을 수 있을 것으로 기대되고 있다.[22]

주민등록제도 자체가 “부동・불온분자의 색출”을 용이하게 하는 데 그 목적을 두고 있는 것이다. 실제 이렇게 만들어진 주민등록제도는 13차의 개정을 거치면서도 그 본래의 모습을 잃지 않고 있다. 가장 대표적인 모습은 주민등록법 시행규칙 제16조이다. 이 조 제1항은 “시장・군수 또는 구청장은 만 17세 이상인 사람이 (……) 주민등록번호를 정정 또는 부여받거나 주민등록 정정신고, 전입신고, 국외이주신고 및 국외이주포기신고 등을 하였을 때에는 지체 없이 그 사항을 경찰청장에게 알려야 한다.”고 규정함으로써 주민등록제도가 법 제1조에서 말하고 있는 “주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것”이라는 입법목적과 다르게 치안유지의 목적으로 이용되고 있음을 잘 드러낸다.

문제는 권위주의체제하에서의 주민등록법 개정이 국민에 대한 통제와 감시를 강화하는 방향으로 이루어졌다는 점 외에도 민주화 이후의 개정 역시 이 권위주의 체제에 대한 교정이나 반성의 모습을 담지 않고 있다는 점이다.[23] 민주화 이후의 주민등록제도의 개정방향은 종래 행정청이 자의적으로 운영해 오던 제도를 법령의 형태로 포섭함으로써 규범적 정당성을 부여하는데 급급하였다. 물론 2012. 6. 1. 주민등록법시행령의 일부개정(대통령령 제23825호)으로 주민등록표에 기재하는 사항에서

있는 암호가 있다, ⑤내년의 정부통령선거를 앞두고 대량의 간첩이 남하한다는 정보가 있다, ⑥병력기피자 단속할 수 있고 시민의 기동을 정리할 수 있다, ⑦선량한 국민으로서 당연히 가져야 한다. 동아일보, 1959. 9. 3. 김영미, 314면

21) 김민호, “정보사회에서 주민등록제도와 개인식별번호체계의 공법적 쟁점,” 공법연구 제40집 제1호, 2011, 372면.

22) 동아일보, 1968. 2. 16. 제1면, “주민등록증 곧 발급”

23) 장종인, 위의 글, 30면

⑩인력동원, ⑫학력, ⑬직업 등의 부분을 삭제함으로써 개인정보수집의 영역은 대폭 축소하였다는 진전은 있었다. 그러나, 그럼에도 불구하고 주민등록번호제에 대한 법적 근거를 마련한다든지 주민등록의 관리를 전산조직에 의하여 할 수 있도록 한다든지 하는 것은 효율성을 강화한 관료화의 결과에 다름 아니다. 나아가 이러한 방치 내지는 규범적 정당화의 작업은 정보통신기술의 발달과 결합함으로써 더욱 커다란 문제만 안겨주고 있다. 즉, 정보통신기술의 발달과 함께 주민등록제도의 문제점이 기하급수적으로 확대되고 있음에도 불구하고 기존의 틀을 완화하거나 제거하지 않고 유지하였다는 점에서 그 폐해를 방치 내지는 방조하였다는 비판을 넘어서기 어렵다. 일종의 부작위에 의한 통제·감시 강화로 나아간 것이다.

이 과정에서 주민등록제도가 정보화와 가장 긴밀하게 유기적으로 결합하는 것을 국가는 방치하게 되었고 오늘날에 와서는 그 폐해와 위험은 제정 당시에는 도저히 꿈도 꾸지 못할 정도로 확산되고 있다.

2.2.2. 국민식별번호: 주민등록번호제도

하지만, 정보화사회에서 무엇보다도 큰 문제로 대두되고 있는 것은 다름 아닌 주민등록번호제도이다. 주민등록법은 "시장·군수 또는 구청장은 주민에게 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다." (제7조제3항)로 하여 모든 국민이 평생동안 바뀌지 않는 단일하고도 유일한 주민등록번호를 부여받도록 강제하고 있다. 그리고 주민(국민)의 관리는 모두 이 주민등록번호에 의거하여 처리하도록 시스템들이 구축되어 있다.

이 주민등록번호는 1968. 9. 16. 개정된 주민등록법시행령(대통령령 제3585호) 제3조에 의해 처음 도입되었다. "간첩이나 불순분자의 색출, 병역기피자의 징병관리 등을 위한 용도"로 도입되었는데, 도입될 당시에도 반대론이 적지 않았다. 당시 제1야당이었던 신민당은 물론 언론에서도 개인의 인격권이라는 헌법상의 권리를 단지 "행정사무의 도구처럼 희생시킨다"는 비판을 제시하였다.[24] 우리 국가가 권위주의 체제로 이행하는 과정에서 반공이데올로기를 빌미로 국가권력의 강화수단으로 주민등록번호제도가 마련되었던 것이다.[25]

주민등록번호의 구성원칙은 이 주민등록번호체제가 단순한 주민관리행정의 보조인자로만 획정된 것이 아님을 잘 보여준다. 그것은 생년월일과 성별(노소 및 내외국인), 주민등록지, 주민등록순서 및 오류검증번호 등으로 구성되는 주민등록번호는 이미 그 번호만으로도 번호의 주체에 대한 일반적 정보와 함께 그 신원을 검증하고 확인하는 수단으로서의 기능을 수행한다. 실제 주민등록번호의 기능을 식별기능, 인증기능, 연결기능, 묘사기능 등으로 분류를 하다고 하면[26] 주민등록번호는 개인에 특정된 번호로서 그 인격을 식별하고 나아가 그 인격의 존재양태(남자/여자, 1900년

24) 이장희, 주민등록번호제에 대한 헌법적 쟁점, 헌법재판연구원, 2013, 8-9면.
25) 윤현식, 개인정보의 국가등록제도와 프라이버시권과의 관계에 관한 연구, 건국대 석사학위논문, 2002, 100-101쪽
26) 이장희, 앞의 글, 12면.

도생/2000년도생, 출생시의 거주지역(소위 고향) 등)를 묘사하는 기능까지 제시한다. 대면적 관계에서 가장 유효한 자기 표시의 수단으로 기능하는 것이다.

아울러 주민행정의 보조인자로서의 성격을 넘어서는 기능은 연결기능에 집중되어 있다. 이미 주민등록관계법령은 주민등록표를 가족관계등록부와 결합하고 있을 뿐 아니라 경찰청의 치안행정에까지 연결하고 있다. 그리고 이러한 연결을 가능케 하는 연결점이 바로 주민등록번호이다. "간첩이나 불순분자의 색출, 병역기피자의 징병관리 등을 위한 용도"라는 본연의 목적이 여전히 주민등록번호제도의 본질을 이루고 있으며, 이는 다시 '휴대폰의 사실상의 실명인증제'를 통해 모바일 내지는 유비퀴터스 소통체제에까지 확장되어 국민의 의사소통에까지 국가의 통제력을 미치게 하는 틀을 이루고 있다.

이러한 주민등록번호제도에 대하여 이은우는 다음과 같은 문제점을 지적한다.

(i) 주민등록번호는 어디에서든 그 사람을 대표하는 유일한 번호로서 그 사람에 관한 모든 개인정보의 통합자와 식별자 역할을 한다.

(ii) 주민등록번호의 구성이 외부에서 그 번호만 보아도 나이, 출신지역, 성별(생물학적인 성) 등을 확인할 수 있게 되어 있어서 인권침해의 소지가 있다.

(iii) 한번 발급된 주민등록번호는 평생 변하지 않는다. 이런 점에서 임의적인 번호체계로 단순한 일련번호에 불과한 번호인 경우나, 번호가 바뀔 수 있는 경우보다 훨씬 더 강력한 전국민 특정번호제도이다.

(iv) 그 동안 수 십년간 축적된 주민등록자료가 전산화되어 있으며, 행정영역의 경우는 모든 행정영역에서 제한 없이 주민등록번호를 식별자로 사용해 왔으며, 민간부문에서도 주민등록번호를 무분별하게 개인식별 수단으로 사용해 오고 있어서 개인정보의 통합화된 정도가 전세계에서 유례를 찾아볼 수 없을 정도로 강력하다. 오늘날 이 주민등록번호는 각급 공공기관에서 보유하고 있는 개인정보화일(중앙행정기관 99종, 지방자치단체 126종, 각급학교 22종, 정부투자기관 기타 204종 : 2000. 12. 행정자치부 공고)과 민간영역에서 보유하고 있는 모든 개인정보의 식별자 역할을 하고 있다. 그뿐만 아니라 최근에는 대부분의 인터넷 웹사이트에서 주민등록번호를 개인의 신분확인용으로 사용하고 있으며, 신용정보회사는 국민들의 주민등록번호를 개인신분확인용으로 사용하도록 데이터베이스로 제공하고 있기도 하다.

주민등록번호는 한 사람에 대하여 그에 특유한 번호 하나가 부여되고(전속성) 그 부여방식은 전국적·전국민적으로 통일된 체계를 이루며(통일성), 결코 중복되지 아니하며(유일성), 일생동안 변하지 않으며(종신성), 모든 정보관리의 기본식별자로 활용되고 있으며(범용성), 모든 국민이 의무적으로 사용하여야 한다(강제성)는 점에서 그 특징이 있다. 아울러 그 자체 개인정보를 담고 있다는 점(개인정보성)도 전세계적으로 유례가 없다. 그리고 바로 이 특징으로 인해 그것은 가장 인권침해적 성향을 가진다.

실제 국가인권위원회의 조사결과에 의하면, 이 주민등록번호는 2005년 현재 법령이 요구하는 법정서식의 47.1%에 달하는 7,648개의 서식이 주민번호를 요구하고 있으며, 공공기관이 사용하는 개인정보파일의 약 80%정도가 사용하고 있다 한다. 민원서식의 경우에는 3,303개중 82%인 2,706개가 주민등록번호를 요구하고 있다. 또한 민간부문의 경우에도 부가통신사업자, 인터넷사업자 등의 경우 2,266개(79.3%)가 주민등록번호를 중심으로 개인정보를 수집하고 있다. 또한 민간부문에서 사용하는 서식 22,872개의 표본을 조사한 결과에 의하면 그 절반 정도가 주민등록번호를 요구하고 있다고 한다.

이러한 조사결과는 그 자체 개인정보 덩어리(생년월일, 성별, 내외국인여부, 주민등록발급지, 발급순서 등)인 주민등록번호가 무차별적으로 수집되고 또 이를 바탕으로 관련된 개인정보가 집중적·통합적으로 관리되고 있음을 보여준다. 즉, 주민등록번호 하나만 있으면 그 소지자에 대한 모든 개인정보를 추적, 수집할 수 있음을 의미할 뿐 아니라, 그의 행적이나 생각, 생활방식, 거래 및 경제활동, 병력, 정부에 대한 사고나 활동(특히 민원서류에서 추적가능한…) 등을 한 눈에 다 파악할 수 있다는 것이다.

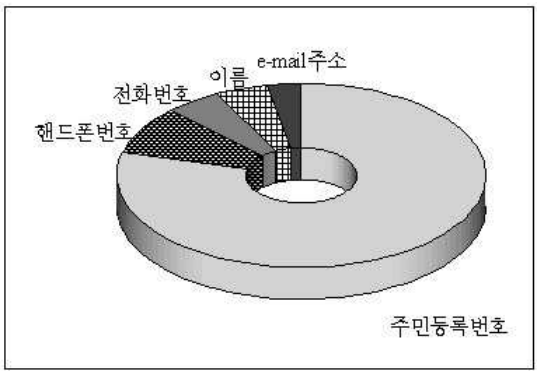


그림 2 가장 입력을 꺼려하는 정보

아래의 그림은 국가인권위원회가 2003년 '금융기관과 인터넷에서의 개인정보 공유현황'에 대하여 네티즌 1,042명을 대상으로 실시한 조사의 결과를 표기한 것이다. 여기서 응답자들은 주민등록번호의 도용 문제에 대해 무려 26.6%가 '주민등록번호가 도용돼 회원가입에 실패한 경험이 있다'고 응답하였다고 한다. 그리고 '인터넷 사이트 회원 가입시 입력을 가장 꺼려하는 정보'는 주민등록번호(75.0%)였으며, 핸드폰번호(8.2%)나 전화번호(4.5%), 이름(4.4%), e-mail 주소(2.8%) 등의 개인정보는 그렇게 강한 거부감을 보이지 않았다.[27]

사정이 이러함에도 불구하고 주민등록번호를 요구하지 못하게 하거나 그 수집을 규제하는 장치는 2011. 9. 30.부터 시행된 개인정보보호법 제24조에 의하여 비로소 가동되기 시작하였다. 하지만 이러한 수집제한조치는 이미 주민등록번호가 사회 일반의 '공유물'이 되어 버린 상태에서 뒤늦게 실시되었다는 점에서 그 조치의 실효성 자체가 의심스러울 지경이 되어 있다. 뿐만 아니라 이런 저런 국가목적을 위

27) 국가인권위원회 2003년 12월 18일자 보도자료 참조. 또한 한국정보보호진흥원이 조사한 다른 자료에서는 주민등록번호를 도용하는 경우 친구의 것을 도용하는 비율이 61.7%이며 주민등록번호생성기 26.7%, 다른 사람 26.7%, 가족 20.0%(중복응답) 등의 순위를 보이고 있다. 이들은 주민등록번호를 도용하는 이유로 '번호유출이 걱정되서'(38.3%) 혹은 '흔적을 남기기 싫어서'(36.7%) 등의 응답을 보인다.(중복응답) 한겨레 2004년 3월 24일자. 이러한 주민등록번호의 남용에 관하여는 이민영, "주민등록번호 남용억제에 관한 법제적 고찰," 정보통신정책 제16권 제8호, 2004 참조.

하여 국가의 법령은 오히려 이를 부추기고 있을 뿐 아니라(특히 각종의 실명제 등), 주민등록번호와 같은 고유식별번호들을 공공기관이 자의적으로 이용하거나 제3자에 제공할 여지를 폭넓게 인정하고 있는 것이 현실이기도 하다.(개인정보보호법시행령 제19조제1항 단서) 나아가 민간부문에 있어서도 경제적 약자일 수밖에 없는 개인의 경우 주민등록번호를 요구하는 강자-기업이나 단체 등-의 명령에 복종하지 아니할 방법도 없는 것이 현실이다. 한마디로 민간부문에서 주민등록번호를 사용하는 것은 오로지 민간의 "자율"에 맡겨져 있다시피 한 것이 현실이다. 2012. 2. 17. 개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 경우 제23조의 2에서 주민등록번호의 사용제한을 규정하고 있기는 하나, 이 또한 너무도 광범위한 예외를 인정하고 있어 개인정보보호의 실익이 의심스러울 뿐 아니라, 그 역시 사후약방문에 불과하다는 비난으로부터도 자유롭지 못 하다.[28)]

스웨덴[29)]이나 미국,[30)] 네덜란드[31)] 등의 개인별번호부여체계와 우리나라의 주민등록번호체계의 본질적 차이는 목적외 사용의 가능성에 있다. 그동안 우리나라의 주민등록번호제도는 1968년 도입된 이래 아무런 제약이나 제재도 없이 민관을 불문하고 자유롭게 사용해 왔다. 앞서 언급한 국가인권위원회의 보고서는 그 단적인 예에 불과하다. 주민등록번호 및 주민등록제도의 목적이 어떠하건 관계없이 개인식별자로서의 주민등록번호의 유효성, 효율성으로 인하여 사람을 대상으로 하는 모든 정보파일은 하나같이 주민등록번호를 중심으로 구성되고 또 이를 기반으로 상호 연동되는 체제를 구축해 왔다. 그리고 이를 위하여 국가영역은 물론 시민사회영역이나 경제영역에서조차 법령[32)]에 의한 강제력을 통해 혹은 관행이나 일방의 요구에 의해

---

28) 또 다른 법제로는 「신용정보의 이용 및 보호에 관한 법률」이 있기는 하나 이는 "주민등록번호를 특별히 보호하는 규정으로 볼 수는 없고, 계속적인 이용을 가능하게 하는 규정이라고 판단된다." 김민호, 382.

29) 스웨덴은 우리 주민등록번호 제도와 유사한 개인식별번호(PIN: Personal Identify Number)제도를 운영한다. 하지만, 이 개인식별번호 제도(10자리 숫자조합)는 사회보장 등 국민의 편의성과 생활 안정 등 사회보장 서비스전달의 효율성을 위한 것으로 사회민주주의체제의 특성으로부터 나온 것이라고 보는 것이 타당하다. 즉, 그 목적과 사용도 등의 면에 있어서는 우리의 제도와는 상당한 거리를 두고 있는 것이라고 보아야 할 것이다. 더구나 스웨덴의 경우 정보통신기술의 발전과 같은 환경변화를 감안하여 1998년 개인정보보호법을 대폭 개정하여 국가에 등록되어 있는 개인정보의 범위 및 용도를 엄격히 제한하고, 그 사용의 필요가 있는 때에는 개인의 명시적 동의를 받도록 명문화해 개인정보의 무분별한 유출을 방지하고 있다고 한다. 김민호 367, 김일환 "住民登錄番號의 違憲性與否에 관한 考察," 헌법학연구 제11권 제3호, 2005, 315-6

30) 미국의 사회보장번호는 개인의 신청에 기하여 발급된다는 점에서 출생과 더불어 그 발급이 강제되는 우리의 경우와는 질적으로 차이가 난다. 프라이버시보호법은, 연방이나 주 정부기관이 사회보장번호를 필요로 하는 때에는 제출의 필수성 여부, 요구의 법률 근거, 제공된 사회보장번호의 사용목적 및 제시거부의 경우 처리방법 등을 미리 고지하도록 하고 있으며, 법령이 정하는 경우를 제외하고는 공공기관이 사회보장번호를 요구하는 것을 금지시키고, 이를 제공하지 않았다는 이유로 서비스 제공을 거부해서는 안 된다는 규정을 두고 있다.(5 U. S. C. Sec. 552a) 서지원, 프라이버시와 국가신분증제도, 서울대학교 석사학위청구논문, 1998, 68쪽.

31) 이러한 미국의 틀은 2007년 11월부터 시행된 네델란드의 시민서비스번호(BSN: Burger Service Number) 제도에도 이어지고 있다. 주로 조세 · 복지 등 공공업무용으로 사용되는 이 시민서비스번호는 개인정보보호법(Personal Data Protection Act)에 의거, 그 사용범위가 엄격히 제한되고 있으며, 개인 사업자 등이 시민서비스번호를 취급할 경우, 사전 허가된 사람만 접근할 수 있도록 철저한 보안시스템의 설치를 의무화하고 있다. 김민호, 365면.

32) 이때의 법령 또한 구체적인 법규명령의 틀 속에서 주민등록번호의 제출을 명하는 것이 아니라, 주로 별

별다른 의식도 없이 주민등록번호가 제공되고 또 이용되어 왔다.

이런 목적 외 사용은 애당초 주민등록번호체계의 도입시부터 예정되어 있다고 해도 과언은 아니다. 우선 그 번호를 방첩과 치안의 목적으로 사용하고자 하는 의도가 명시되었을 뿐 아니라, 이를 주민등록증에 명기하도록 함으로써 행정내부적인 편의를 위한 분류번호체계의 수준을 넘어 언제든지 그 사람의 신원을 확인하고(식별기능), 나아가 각종의 데이터베이스와 연동시키거나 혹은 새로운 개인정보파일을 자유롭게 창출할 수 있도록 하는 목적(연결기능)것이다.

이 점은 주민등록번호제도가 현재의 시점에서 이용되는 양상과 직결된다. 공공기관에서의 주민등록번호는 일반적인 식별자 및 연결자로서의 기능을 넘어 국가가 상정하는 가장 추상적 수준의 위험을 '예방'하고 '추적'하는 기능을 수행한다. 아직도 공직선거법상에 남아 있는 통신실명제나 휴대폰 개통시 주민등록번호의 수집을 허용하는 체제는 그 대표적인 예이다. 헌법상 보장되는 표현의 자유에도 불구하고 그것을 야기할 수 있는 체제위험이나 도덕률 침해의 문제를 사전에 제시하면서 그러한 위법을 적발하고 추적할 수 있는 장치(혹은 이러한 추적의 위협으로 일반예방을 수행하고자 하는 장치)로서 활용되는 것이 통신실명제이다.[33] 위험이 발생할 수 있는 구체적인 인자들을 지적함이 없이 막연한 상황이나 맥락만으로 일정한 위험을 추상화해내거나 혹은 어떠한 상황인자들을 결합하여 미래의 특정한 조건하에서 어떠한 현상이 발생할 수도 있음을 예측하고 이에 기반하여 사회질서에 대한 위험을 도출하는 한편, 국가는 이를 사전에 예방하고 통제하여야 할 의무와 권한을 가지는 것으로 규정하는 일종의 예방형법 혹은 예방경찰의 현상이 이에 해당한다.[34] 나타나고 있으며 이를 가능하게 하는 가장 유효한 장치중의 하나로 주민등록번호가 활용되는 것이다.

주민등록번호제도가 국가주의의 전형적인 예에 해당한다고 보는 것은 바로 이 때문이다. 국가의 행위영역 상대편에 국민 개개인의 기본권과 권리를 상정하는 것이 아니라, 국가의 고권적 권력에 복종하는 국민만을 설정하고 그 통제의 기제로서 주

표상의 서식을 통하여 암묵적으로 주민등록번호의 기재를 요구하는 방식을 사용해 왔다. 개인의 기본권을 제한하면서 암묵적이고도 우회적인 방법을 사용해 온 것이다. 헌법재판소는 "[주민등록법] 시행령조항에서는 주민등록법 제17조의8 제5항의 위임규정에 근거하여 주민등록증발급신청서의 서식을 정하면서 보다 정확한 신원확인이 가능하도록 하기 위하여 열 손가락의 지문을 날인하도록 하고 있는 것이므로, 이를 두고 법률에 근거가 없는 것으로서 법률유보의 원칙에 위배되는 것으로 볼 수는 없다." (헌법재판소 2005. 5. 26. 99헌마513등)고 하여 이러한 편법적 기본권제한의 관행들을 정당한 것으로 인정하고 있다.

33) 이에 관하여는 한상희, "음란물 규제법제와 통신실명제," 정보법학 제3호, 1999, 361-386면 참조.

34) 이러한 국가주의적 경찰국가의 모습은 나치형법체계에서 가장 잘 드러났었다. 사회질서의 유일한 보장자・실천자로서의 국가는 일정한 신조나 경향만으로도 반사회적 위험을 규정할 수 있게 되고(혹은 있어야 하고), 개인은 민족공동체개념으로 구성되는 국가를 위하여 자기의 자유와 권리에도 불구하고 국가의 이러한 위험예방적 조치에 복종하여야 할 것을 요구하였던 것이다. 한마디로 "모든 국민은 자신과 자신의 삶을 '민족 전체에 대한 봉사'라는 관점에서 바라보아야 하며, 개인의 자유는 전체를 위해 언제든지 제한될 준비가 되어 있어야 했다." 윤용선, "나치의 범죄정책: 남성 동성애 사례를 중심으로," 역사와문화 제13호, 2007, 84-104면. 권위주의체제에서의 우리 국가도 마찬가지의 위험을 제시하며 사회와 개인을 통제하였고, 그러한 국가주의적 경찰관행은 서울광장에의 통행권제한 사건에서 보듯 여전히 지속되고 있다.

민등록번호가 활용되고 있는 것이다. 환언하자면 주민등록번호제도를 구성한다고 일컬어지는 행정편의주의는 단순한 행정효율성의 문제에 한정되는 것이 아니라, 국가에 의하여 일방적으로 규정되는 행정가치와 관료적 편의에 의하여 결정되는 행정수단은 언제나 국민의 권익 위에 존재하며 국민은 이를 위하여 자신의 권리와 이익을 포기할 것이 강요되는 국가주의적 체제의 문제가 표출되는 하나의 양상에 불과한 것이다.

민간영역에서 주민등록번호의 사용이 관례가 된 것은 이러한 국가행태에서부터 비롯된다. 공공영역에서 사용되는 주민등록번호는 마찬가지로 거래의 상대방의 신원을 식별하는 수단으로 최적의 인자가 되어 있으며, 나아가 연결자로서도 가장 효율적이고도 효과적인 것이 되어 있었던 것이다. 뿐만 아니라 국가에 의하여 정례적으로 이루어지는 각종의 검색·검속-예컨대 정보통신망사업자에 대한 통신기록의 요구 등-에 대응함에 있어서도 저렴하고도 효과적인 수단이 될 수 있었다. 게다가 주민등록번호는 한번 부여받으면 어떠한 경우에도 변경할 수 없다는 불변성, 항구성을 가진다. 그를 바탕으로 구축되는 데이터베이스의 효율성을 최대화하고 있는 것이다.[35]

3. 주민등록번호제도의 위헌성

3.1. 주민등록번호제도의 헌법침해

3.1.1. 심사기준

우리나라의 주민등록제도는 반공냉전이데올로기를 기반으로 한 권위주의체제의 구축 수단으로 구성되었던 그 출발점에서부터 정보사회에서 수많은 개인정보와 연동됨으로써 개인의 생활관계 자체를 침해하는 상황에 이른 지금에 이르기까지 수많은 비판과 도전을 받아왔다. 주민등록번호제도가 처음 도입될 때 그 반대론은 개인에게 번호를 붙여 호명함은 그의 인격을 침해하는 것이라는 이유를 들었다. 개인의 인격권 및 그 근거로서의 존엄권을 침해하는 것이라 보았던 것이다. 하지만, 오늘날과 같은 정보사회에 있어서는 주민등록번호제도는 개인정보자기결정권에 대한 직접적 침해 혹은 제한으로 규정하여 크게 무리하지 않다.[36] 즉, 주민등록번호제도는 생년월일 등의 개인정보를 수집하여 숫자의 조합의 형태로 가공하여 분류하고 이를 주민등록증에 기재함으로써 외부에 노출하는 한편 다른 개인정보와 연동시킬 수 있는 가능성을 열어둔다는 점에서 개인정보자기결정권과 직접적인 연관을 가진다.

---

35) 이 점은 후술하듯 주민등록번호제도가 가지는 최대의 문제점이다. 자신의 주민등록번호가 유출되어 지금까지 축적된 자기 개인 정보가 온전히 다 노출되었음을 넘어, 미래의 개인정보까지도 유출될 가능성이 명확함에도 불구하고 그 당사자(뿐 아니라 국가까지도)는 이 주민등록번호를 변경할 수 없는 상황이 벌어지고 있는 것이다.

36) 주민등록제도 그 자체의 유효성에 대한 거의 유일한 헌법판단인 주민등록법 제17조의8등 위헌확인사건(지문날인 및 지문정보의 경찰청보관·처리행위의 위헌확인사건: 헌법재판소, 2005. 5. 26. 99헌마513등)에서도 헌법재판소는 이 문제를 개인정보자기결정권의 맥락에서 다루고 있다.

문제는 이렇게 개인정보자기결정권을 제한하는 주민등록번호제도의 위헌성여부를 판단하는 심사의 기준을 어떻게 설정하여야 할 것인가라는 점이다. 이와 관련하여 우리 헌법재판소는 "그런데 이 사건은 (……) 개인의 본질적이고 핵심적 자유영역에 속하는 사항이라기보다는 사회적 연관관계에 놓여지는 경제적 활동을 규제하는 경제사회적인 입법사항에 해당하므로 비례의 원칙을 적용함에 있어서도 보다 완화된 심사기준이 적용된다고 할 것이다"[37]라고 함으로써 독일의 경우와 같이 개인의 핵심적 자유영역에 대하여는 엄격한 심사기준을 적용할 것을 밝히고 있다.

오늘날과 같은 정보사회에서의 개인정보자기결정권은 이런 맥락에서 엄격한 심사기준이 적용되어야 할 기본권영역에 속한다. 그것은 개인의 사적 영역에서 그의 인격과 사적 생활이 구성되고 또 보호되는 핵심요소를 이룬다. 통상적으로 민감정보(sensitive information)라 불리는 정보영역은 그 대표적인 예이겠으나, 그 외에도 수많은 개인정보들이 상호 결합되는 과정에서 이러한 민감정보를 추출할 수 있는 가능성을 내포하게 된다.[38] 그리고 바로 이 점에서 일부의 개인정보 혹은 개인정보의 결합정보에 대한 정보주체의 통제권은 자신의 자기운명결정을 위한 기본적인 전제를 이룬다. 민주주의의 기초라 할 수 있는 자기지배의 생활영역이 형성되는 본질적 요소가 되는 것이다.

주민등록번호제도는 이 점에서 가장 본질적이고도 핵심적인 자유영역과 관련을 가진다. 그것은 그 자체 개인정보를 담고 있는 것일 뿐 아니라, 그의 사적 생활을 판별하는 인식자로서의 기능과 함께 그의 사적 생활영역의 모든 것을 규정하고 구성하는 개인정보를 추출할 수 있는 연결자로서의 기능을 수행하고 있기 때문이다.[39] 환언하자면 그것은 개인의 인격발현과 개성신장의 불가결한 부분에 관한 정보 내지는 정보연결자로서의 성격을 가지고 있는 것이며, 이에 그 위헌성에 관한 심사는 보다 강화된 엄격한 심사기준에 의하여야 한다.

3.1.2. 목적의 정당성

전술하였듯이 주민등록번호제도는 두 가지의 목적을 가진다. 그 하나는 명시적 목적으로 "주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것(주민등록법 제1조)"을 들 수 있다. 또 다른 하나는 헌법재판소도 인정하였듯이 "간첩이나 불순

37) 헌법재판소 2005. 2. 24. 2001헌바71. 이러한 판단은 직업선택의 자유와 관련하여서도 이어져 헌법재판소는 "핵심적 자유영역에 대한 침해"인가의 여부로써 그 심사의 강도를 정하고 있다.(헌법재판소, 2002.10.31. 99헌바76등) 즉, 생명권이나 신체의 자유, 사적 영역의 보호, 개인의 인격권 등의 본질적·핵심적 자유는 물론, 여타의 자유권의 경우에도 그것이 사회적 연관성이나 사회적 기능보다 개인의 자유실현의 물질적 기초가 되거나 혹은 개성신장의 불가결한 요소일 경우에는 보다 강한 헌법적 보호를 받는 것으로 이해하고 있다.

38) 예컨대 교원의 봉급명세서에는 정당이나 사회단체에 대한 당비나 기부금의 지급명세가 담겨 있어 민감정보를 알 수 있는 단서가 되며, 한 개인이 포털의 뉴스제공서비스에 접속한 로그기록들은 종합적으로 그 사람의 정치적·종교적 성향을 알 수 있는 빅데이터를 구성하게 된다.

39) 개인정보보호법이나 정보통신망법 등에서 최근 법개정을 통하여 주민등록번호의 수집을 제한하고자 한 것도 정보사회에서 주민등록번호의 수집으로 인하여 개인의 사생활을 본질적으로 침해될 수도 있음을 자각하였기 때문이다.

분자를 용이하게 식별 색출하여 반공태세를 강화”하는 방첩과 치안목적이라는 묵시적·입법사적 목적을 가진다. 이에 이러한 목적은 헌법 제37조 제2항에 의한 목적 정당성의 원칙에 부합한다는 의견도 없지 않다.[40] 냉전적인 반공국가의 체제를 기반으로 형성된 우리 국가체제를 감안할 때 이러한 의견의 타당성을 부인할 수는 없다. 하지만, 그러한 목적정당성의 판단은 주민등록제도에 대한 경우라면 몰라도 주민등록번호제도에 관한 한 그의 본질적 기능을 축소왜곡하는 것이라는 점에서 심각한 오류에 빠진다.

주지하듯, 주민등록번호는 네 가지의 기능을 지향한다: 식별기능, 인증기능, 연결기능, 묘사기능이 그것이다. 여기서 위의 두 목적에 봉사하는 기능은 식별·인증기능과 묘사기능뿐이다. 오늘날 광범위하게 사용되고 있는 연결기능은 전체 국가행정의 영역과 관련시켜 볼 때 주민등록번호제도의 가장 본질적 기능으로 고양되어 있음에도 불구하고 그것은 주민생활의 편익증진이라든가 혹은 대간첩·치안목적과는 거리가 있다. 특히 그러한 주민등록번호가 민간영역에서까지 폭넓게 사용되도록 방임함으로써 가장 보편적인 연결자로 기능하고 있는 현실은 이러한 입법목적 이외의 현상이기도 하다. 환언하자면 현재의 주민등록번호제도는 그 입법 당시 추구하였던 입법목적을 넘어서서 개인정보의 연동이라든가 민간이용에까지 확장된 광대역의 목적에 봉사하는 양상을 보인다.[41]

더불어 주민등록법 제1조에서 “주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것”을 편익증진과 행정사무적정처리라는 두 가지의 목적을 열거한 것이라고 본다면 이 “행정사무의 적정 처리”라는 입법목적이 과연 기본권 제한의 정당한 사유로 인정될 수 있을런지도 의문이다. 헌법 제37조제2항에서 열거하는 국가안전보장, 사회질서유지 및 공공복리의 증진과 거리가 있는 단순한 행정편의주의의 표현에 불과하기 때문이다. 만일 그것을 편익증진을 위한 행정사무의 적정처리라는 하나의 목적을 제시한 것이라고 한다면 주민편익증진과 무관하게 진행되고 있는 각종의 개인정보 연결자로서의 주민등록번호의 기능은 목적 외의 것이 되고 만다.[42]

3.1.3. 수단의 적합성

주민등록번호제도의 수단적합성 판단에서도 동일한 오해가 존재한다. 일설에서는

---

40) 고문현 외, 국가신분확인체계 발전방안연구, 행정안전부연구용역보고서, 한국비교공법학회, 2010. 92면

41) 실제 주민등록법은 주민등록번호의 용도를 개인별 주민등록표의 정리(주민등록번호순: 제8조), 주민등록증기재를 통한 신원확인(제24조제2항), 국가기관등에서의 신원확인(제25조), 주민등록사항의 진위확인(제35조) 등으로 열거하고 있다. 주민등록번호제도의 입법목적을 식별자 및 인증자에 한정하고 사법경찰관리의 직무와 관련하여 예외적으로 대면관계에서 본인을 확인하거나 조회하기 위한 묘사기능을 추가하고 있을 따름이다. 하지만 오늘날 주민등록번호가 가장 많이 활용되고 있는 연결자로서의 기능은 주민등록법 그 어디에도 존재하지 않는다.

42) 실제 주민등록법은 주민등록증의 발급주체를 시군구청장으로 하고(법 제24조제1항) 사무의 관정 역시 지방자치단체에 두고 있으나(법 제2조) 실질적으로는 행정안전부의 총괄지휘를 받도록 하고 있는(법 제3조) 이중적 구조를 가지고 있다. 즉, 목적이 “주민생활의 편익”에 놓여지기는 하지만, 그 실체에 있어서는 ‘국민’ 통제의 수단임을 간접적으로 보여준다.

“그 조치나 수단이 목적달성을 위하여 유일무이한 것일 필요는 없는” 것이라는 헌법재판소의 결정을 인용하면서 주민등록번호의 부여를 통해 범죄예방이나 범인의 검거, 행정사무의 적정하고 간이한 처리 등의 공익에 봉사하고 있음을 들어 그 수단적합성의 판단에 긍정적 입장을 내어놓고 있다.[43] 하지만 지금 문제로 되고 있는 것은 무색무취의 주민등록번호의 부여라는 수단이 아니라 전속성・통일성・유일성・종신성・범용성・강제성을 갖추고 일정한 개인정보까지 담고 있는 주민등록번호를 부여하고 있다는 현실이다. 비록 헌법재판소에서 수단적합성에 관한 판단은 거의 형식적으로 운영되고 있기는 하지만, 그럼에도 불구하고 주민등록번호가 가지는 이러한 속성들이 위에서 열거한 목적의 달성의 위해 어떠한 유효성을 가지고 있는지를 판단하여야 한다. 특히 생애주기를 걸쳐 어떠한 변화도 인정하지 않는 종신성과 같은 속성이 이런 행정목적의 달성에 어떻게 유효하게 기여할 수 있는지에 대한 판단은 반드시 짚고 넘어가야 할 부분이기도 하다.

3.1.4. 피해의 최소성 및 법익균형성

엄격한 심사기준은 주로 피해의 최소성이나 법익균형성에 대하여 작용한다. 즉 달리 가벼운 제한의 방법이 있다면 그 방법을 취하여야 하며, 공익과 사익의 균형 판단도 보다 엄격하게 이루어진다. 주민등록번호제도에 관한 한 이 부분의 판단은 무엇보다 그 범용성에 주목하게 된다. 개인이 이용할 수 있는 자기식별번호로서는 주민등록번호 외에도 “운전면허번호, 의료보험번호, 여권번호, 인사번호, 학번, 예금계좌번호, 신용카드번호 등” 다양한 번호가 있다.[44] 하지만 그럼에도 불구하고 주민등록번호는 이 모든 생활영역에서 무차별적으로 통용되는 유일한 개인식별번호로 제도화되어 있다. 심지어 이상의 개인별 번호들을 연동시키는 보편적 연결자로서 기능하기까지 한다. 대안적 수단이 광범위하게 존재함에도 불구하고 주민등록번호제도는 가장 침해적인 방법으로 개인의 자기정보결정권을 제한하고 있는 것이다.

물론 이러한 범용성 및 보편성으로부터 파생되는 위험을 예방하기 위하여 주민등록법은 주민등록번호의 무단생성이나 부정사용 등을 형사처벌하고 있기는 하지만,[45] 그것만으로 피해의 최소성을 확보하기 위한 입법적・제도적 방비가 이루어졌다고 할 수는 없다. 다른 어떠한 법리적 판단에 선행하여 지금 현재 개인의 주민등록번호가 중국등 외국에까지 누출되어 각종의 사기행각에 활용되는 지경에 이르고 있는 현실[46]만으로도 이러한 위험방지책의 허구성을 잘 알 수 있을 것이다.

뿐만 아니라 합헌론이 들고 있는 다양한 행정적 수요에 대한 봉사라는 법익 또한 주민등록번호제도의 본원적 속성-전속성・통일성・유일성・종신성・범용성・강제성-과 무관하게 이루어지는 것이 대부분이다. 국방, 치안, 조세, 선거, 사회복지 등의

43) 고문현 외, 위의 글, 92-3면.
44) 고문현 외, 위의 글, 93면.
45) 고문현 외, 위의 글, 93면.
46) 대체로 주민등록번호의 유출로 인한 2차피해로 거론되고 있는 것은 명의도용, 개인정보불법유통, 스팸, 피싱 등이다. 성균관대학교 산학협력단, 주민등록번호제도 개선방안연구, 국가경쟁력강화위원회, 2009. 11. 98면 참조.

영역은 그 각각에 특유한 개인식별번호를 사용하거나 혹은 '무색무취'의 개인식별자를 이용함으로써 충분히 그 목적을 이룰 수 있다. 환언하자면 주민등록번호를 하나의 일련번호라는 내부적 분류코드로 규정하지 아니한 채 개인의 인격 전체를 대표하는 가상의 인격으로 고양시켜 놓은 것에 상응하는 공익은 어디에도 존재하지 않는 것이다.[47] 아울러 현재 널리 도용당하고 있는 주민등록번호로 인하여 자신의 모든 생활영역에서 불안에 빠질 수밖에 없는 사람들의 피해를 감안한다면 어떠한 논거로서도 법익의 균형성 심사를 통과하기 어려울 것이다.[48]

3.1.5. 입법체계의 문제: 포괄적 위임입법

주민등록법에서 주민 개개인에게 일정한 고유번호를 부여하는 제도 자체는 외국의 예에서도 보듯 그 위헌성을 판단하기가 쉽지는 않다. 다만 현행의 주민등록번호 제도는 그 고유번호에 일정한 속성-전속성・통일성・유일성・종신성・범용성・강제성-을 부여하고 이를 행정내부적 목적으로만 사용하는 것이 아니라 외부적 목적에도 활용할 수 있도록 함으로써 식별자, 인증자의 기능 외에도 연결자로서의 기능을 수행하게 만들었다. 한마디로 개인정보자기결정권을 제한하는 중요한 인자로 주민등록번호를 구성하고 또 활용하고 있는 것이다.

하지만, 이러한 기본권 제한적 제도가 입각하고 있는 법률적 근거는 거의 없다. 주민등록법 제7조 제3항과 제4항은 "주민에게 개인별로 고유한 등록번호를 부여"할 것만 규정한 채 그 번호를 부여하는 구체적인 방법은 대통령령으로 위임하였고, 대통령령 제7조제4항은 이를 다시 시행규칙으로 위임해 버렸다. 유일하게 주민등록법에서 주민등록번호를 규율하고 있는 조항은 제24조 제2항으로 주민등록증 기재사항 중에 하나로 주민등록번호를 열거하고 있을 따름이다.

주민등록법의 이러한 규정방식은 국민의 기본권 실현과 관련된 영역에서는 항시 의회유보의 원칙이 적용될 것을 요구하고 있는 헌법의 명령에 위반된다. 주민등록번호가 가지는 기본권의 제한적 성격을 법률의 차원에서 규정하지 아니한 채(법률유보의 위반), 대통령령에 포괄적으로 위임하고(포괄적 위임금지 위반), 나아가 그조차도 곧장 시행규칙으로 재위임해 버리는 우를 범하고 있는 것이다. 더구나 주민등

47) 사실 이런 논리는 '국가적으로 선인 것은 헌법적으로도 선이다'라는 철저한 국가주의적 명제의 단순반복에 불과하다. 근대입헌주의 이래 국가는 절대적 선의 영역에서 떠나 헌법적 가치에 종속되는 하위개념으로 상정된다. 즉, 권력의 통제와 국민의 기본권보장이라는 보다 상위의 가치에 국가가 봉사하여야 하는 것이 곧 근대입헌주의의 본질적 이념이다. 그리고 이 관점에서 본다면 비록 행정적 편의가 증진되었다 하더라도 그것이 국민의 기본권에 어떠한 영향을 미친다면 그 편의를 후자의 입장에서 재심사하고 재평가하는 것이 필요하다.

48) 엄밀히 보자면 합헌론 역시 결론에 이르러서는 주민등록번호제도의 한계를 인정하고 있다. 특히 이들은 범용성과 종신성 등에 관하여는 "주민등록번호 자체의 위헌성과 별개로"라는 전제하에 제도의 수정을 촉구하고 있다. 다만 이들이 합헌론의 논거로 제시하고 있는 "그와 같은 문제는 주민등록번호의 무분별한 활용을 허용하고 있는 법제도나 사회적 현실에서 비롯되는 것이지 주민등록번호 그 자체의 고유한 문제라고 보기는 어렵다"라는 판단(위의 글, 94면)은 상당히 문제적이다. 제도를 그 맥락에서 떼어 놓고 현실적 한계를 제도의 하자와 분리시키는 입장은 결국 입법자의 무한정한 입법형성권을 그대로 승인하는 것에 다름 아니기 때문이다. 헌법재판소가 동성동본금혼제도에 대해 위헌선언을 한 것도 제도 자체의 고유한 문제를 이유로 한 것이 아니라 시대변화에 따른 그 목적의 타당성상실을 이유로 하였다. 헌법재판소, 1997. 7. 16. 95헌가6 참조.

록번호에 의하여 제한되는 개인정보자기결정권에서 가장 필수적인 요소라 할 수 있는 자기정보통제권-정정권, 변경권, 삭제권 등-에 대해서는 아무런 규정조차 두지 않음으로써 철저한 입법상의 직무유기를 범하고 있다.

결국 이렇게 보면 현행의 주민등록제도는 완벽하게 위헌적인 것이 되어 버리고 만다. 김민호[49]의 말처럼 "도입 당시인 1960년대와 1970년대에는 현재와 같이 국가권력이 헌법과 법률에 구속된다는 법치주의 원칙이 제대로 확립되어 있지 않았던 시기였기 때문에 이러한 법률이 국민의 기본권을 침해하는지에 대해서는 제대로 검증할 기회도 없이 입법된 것으로 보인다"고 구차한 변명을 할 수는 있을지나, 그것으로 이러한 위헌성을 가릴 수는 없다.[50]

3.1.6. 보 론

누차 언급되었듯이 오늘날 주민등록번호를 중심으로 구성되는 개인정보는 그 자체 중요한 상품이 되어 커다란 시장을 형성하고 있다. 최근만 하더라도 2004. 5. 리니지2 가입자 8,500명의 개인정보가 유출된 것을 비롯하여 2006. 3. 국민은행의 고객정보 3만여건이 공개되었으며, 이듬해에는 국민건강보험공단에서 72만여명의 개인정보가 유출되기도 하였다. 2008. 2.에는 옥션경매사이트와 하나로텔레콤에서 각각 1천만명과 6백만명의 고객정보가 유출되었고, 2008. 9.에는 GS칼텍스의 고객정보 1,100만건이 유출되기도 하였다.[51] 2011년에도 SK나 넥슨 등에서 각각 3,500만건 및 1,320만건의 정보가 유출되었다. 그리고 이러한 개인정보의 핵심에는 언제나 주민등록번호가 존재한다. 그것은 모든 것에 관련된 범용적 식별자이자 동시에 모든 것을 연결하는 보편적 연결자로서 기능하는 만큼 무엇보다도 부가가치가 높은 개인정보이기 때문이다.

49) 김민호, 앞의 글, 372면

50) 이희훈, "주민등록번호에 대한 헌법적 고찰 - 개인정보자기결정권의 침해를 중심으로," 토지공법연구 제37집 제1호, 2007 참조.

51) 성균관대학교산학협력단, 위의 글, 97면.

피해구분		이용정보	피해유형
명의도용	인터넷회원가입	성명, 주민번호	· 회원가입 가능한 사이트에 타인명의 회원가입 · 사이버머니 취득 후 판매
	기존회원 자격도용	ID, PW, 성명, 주민번호	· 회원자격 도용 · 타인명의 비방글 게시
	신분증 위조	성명, 주소, 주민번호	· 타인명의 각종 신분증 위조(2차 유출시 재산피해가 큼) · 위조신분증으로 타인명의 부동산 절취 · 불법취업 등 신분 위장
	오프라인서비스 명의도용	성명, 주소, 주민번호, 계좌번호	· 타인명의 금융계좌 및 휴대폰 개설 · 증권사 CMS 계좌이체로 금전 탈취 · 보이스피싱용 대포통장 판매 · 타인명의 대포차 할부구매후 판매
개인정보 불법유통	개인정보불법유통	모든 개인정보	· 통신사 영업점, 스팸발송업자, TM업자 등에게 판매되어 이용
	인터넷 유포	모든 개인정보	· 개인정보 판매 목적
스팸	불법 스팸발송	이메일, 전화번호	· 불법 스팸 및 TM 발송에 이용
피싱	보이스피싱	성명, 전화번호	· 기관사칭 전화사기, 납치사칭 전화사기 등에 이용

그리고 이렇게 유출된 개인정보는 또 다른 제2차 피해를 양산한다. 전술한 바 있지만 중복의 우려를 무릅쓰고 인용하자면 다음의 표와 같다.[52] 실제 그동안 알려진 개인정보유출 건수만 하더라도 그 합계가 우리 국민의 총수를 넘어선다는 보도도 있다. 이것이 사실이라면 거의 모든 국민이 주민등록번호를 유출당한 채 전생애에 걸쳐 전방위적 피해 또는 그 가능성에 고통을 받아야 하는 것이다. 게다가 하지만, 그럼에도 불구하고 이러한 피해를 교정하거나 예방할 수 있는 길은 아무데도 없다. 통상적으로 주민등록번호제도의 대안으로 I-PIN의 사용과 같은 방법을 거론하기는 하지만, 그것은 미래를 향하여 나의 주민등록번호와 그에 기반한 나의 개인정보를 보호할 수 있는 방안에 관한 것이지 이미 유출되어 다른 사람의 수중에 들어가 있는 나의 개인정보와 그 주민등록번호의 해악성을 교정할 수 있는 방안은 아니다. 나아가 I-PIN제도가 유효성이 검증된다 하더라도 그것 또한 주민등록번호에 기반한 본인확인에 터잡고 있는 만큼 유출된 나의 주민등록번호로써 새로운 I-PIN을 만들어 내거나 혹은 나의 I-PIN을 무효화하는 가능성도 없지 않다.

하지만, 우리의 주민등록법제는 이렇게 이미 유출되어서 각종의 제2차 피해의 잠재성을 구축하고 있는 주민등록번호와 그 해악성에 대한 대책은 전혀 마련하고 있지 않다. 일종의 국가적 부작위로 일관하고 있는 것이다. 그리고 바로 이 점에서 이 글의 출발점이 되었던 헌법소원심판청구사건-주민등록법 제7조제3항 및 제4항의 위헌을 구하는 사건-은 의미를 가진다. 국가목적의 수행을 위하여 국가의 입법 및 집

52) 위의 책, 98면

행작용에 의하여 유발된 위험-주민등록번호의 유출로 인한 제2차 피해의 발생위험-은 그 인과의 관계뿐 아니라 발생의 과정과 양상에 있어서도 명약관화 격이다. 주민등록번호를 유출시킨 것은 주로 사기업이지만 그러한 위험 자체를 야기한 것은 주민등록번호제도를 창출하고 운용하여온 국가이다. 국가의 부작위에 대한 책임을 추궁할 수 있다는 것이다.

물론 이때의 책임은 국가배상의 수준에 이르지는 못 한다. 주민등록번호를 수집하고 관리해온 사기업의 책임이 그 인과의 연결을 단절시키기 때문이다. 하지만, 국가의 입법교정의 책임은 의연히 존재한다. 더 이상의 위험을 방비하고 이미 발생된 위험을 제거하기 위한 추상적이고 일반적인 교정책을 마련하여야 할 책임이 있는 것이다. 그리고 그 중의 가장 손쉬운 방법이 주민등록번호의 유출을 당한 주민에게 그의 주민등록번호를 변경해 주는 것이다. 이는 이미 불법의 가능성에 노출된 자신의 아이덴티티를 변경함으로써 그 불법의 가능성으로부터 벗어날 수 있도록 한다.[53] 하지만, 안전행정부는 물론 지방자치단체조차도 이러한 주민등록번호의 변경을 위한 법적 근거가 없다는 이유로 그 신청을 거부하였다. 국가에 의하여 위험이 발생하였고 그 위험에 의한 직접적 피해를 입고 있거나 입을 가능성에 처한 사람에 대해 국가는 입법의 불비를 거론하여 책임을 회피하고 있는 것이다. 문제는 이러한 피해에 직면한 사람이 거의 전 국민적 규모에 이르고 있다는 점이다. 그 피해는 개별적·특수적 피해가 아니라 일반적·보편적 피해이며 추상적·잠재적 피해가 아니라 지금 현재화되어 있는 구체적인 피해임에도 불구하고 국가는 직무유기로만 일관하고 있을 따름이다.

이 사건에서 위헌판단이 절실함은 바로 이 때문이다. 그것은 정보사회라는 현상황에서 주민등록번호제도가 안고 있는 본질적 하자로 인한 것이기도 하지만 동시에 국민 대다수가 지금 현재 처해 있는 법적 불안을 제거하여야 한다는 국가적 책무로부터도 연유하는 것이기도 하다.

53) 실제 개인식별수단으로서의 주민등록번호제도의 대안으로는 그 수단의 다양화가 최우선적으로 꼽힌다. 여권이나 공무원증, 학생증 등과 같이 공인된 기관에 의하여 발부된(그러나 그에는 주민등록번호가 기재되지 아니한) 신분증으로 그를 대신하도록 법제를 정비하여야 한다는 것이다. 주민등록번호의 종신성을 해체하고 필요한 때에 주민등록자의 요구에 의하여 주민등록번호를 변경할 수 있도록 하는 것은 또 다른 측면에서의 개인식별수단의 다양화에 해당한다. 엄밀히 보자면 그러한 변경제도를 도입함으로써 지나치게 많은 의존의 대상이 되었던 주민등록번호제도가 서서히 해체될 수 있는 시간적·상황적 여건을 조성하는 과도기를 구성할 수 있게 되기도 한다.

Ⅲ. 인터넷실명제

1. 인터넷상의 본인확인

이상과 같은 문제점과 위헌성을 내포하고 있는 우리나라 주민등록번호제도는 이제 인터넷상의 의사소통까지 통제하는 수단으로 작용한다. 인터넷상의 의사소통이 이루어지는 과정에서 그 통신자의 실명 또는 본인성을 확인하도록 강제하는 장치가 시행되고 있기 때문이다. 사이버공간에서의 익명성이 지나친 해방감을 부여하여 무책임한 발언이나 명예훼손・모욕, 타인의 권리침해 혹은 유언비어나 허위사실유포 등의 폐해를 드러내기도 한다는 점을 우려하여 인터넷상에서 통용되던 익명성을 규제하고자 한 것이다. 그 출발은 1998년 12월7일 정보통신부의 발표에서부터 비롯된다. 정보통신부는 정보통신망 이용자들이 건전한 정보를 손쉽고 빠르게 이용할 수 있도록 하기 위해 PC통신과 인터넷 등 온라인서비스를 이용하려면 반드시 실명으로 가입해야 하고, 기존 가입자도 주민등록번호와 성명이 맞지 않으면 강제 해지된다는 것을 골자로 하는 '온라인서비스 이용증진방안'을 마련, 발표한 바 있다.[54] 또한 2003년에는 정부부처가 개설한 게시판 등의 경우 "인권 침해와 명예 훼손 등을 막기 위해" 주민등록번호와 성명으로 실명을 확인받은 자만이 이용할 수 있도록 하는 방침을 추진하였음[55]은 이의 대표적인 예이다.

하지만 이 당시에도 수많은 찬반의 논란들이 있었음에도 불구하고 2007. 1. 26.「정보통신망이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 제44조의 5로 도입되어 시행되었다.[56] 이 규정은 게시판을 설치・운영하는 자는 그를 이용하려는 자의 본인 확인을 위한 조치(이하 "본인확인조치"라 한다)를 취하도록 강제하면서 그 대상을 ①국가기관, 지방자치단체, 공기업・준정부기관, 지방공사・지방공단(이하 "공공기관등") 등과, ② 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 10만명 이상이면서 대통령령으로 정하는 기준에 해당되는 자로 하였다. 하지만 이러한 규율은 2012. 8. 23. 헌법재판소에 의하여 그 일부(위의 ②부분)가 위헌으로 선언되면서 그 효력을 상실하였다.[57]

인터넷실명제에 관한 이런 일련의 경과는 정보사회에 있어서의 개인정보수집행위

54) 정보통신부 보도자료(1998.12.04) 경향신문, "PC통신・인터넷 가입 실명제," 1998. 12. 7일자 22면.

55) 실제 2003년초 현재 이러한 실명제는 18개 중앙 정부 부처 중 9개 부처에서 실시되고 있는 바, 정보통신부는 그것을 모든 부처로 확대한다는 것이다. 중앙일보 2003.3.28, http://news.naver.com/news_read.php?oldid=20030328000045052201 2&s=6&e=245. 이에 발맞추어 그 당시 개정되었던 주민등록법은 소위 주민등록번호생성기 등을 이용하여 주민등록번호를 위조하는 것을 금지함으로써 통신실명제를 향한 강제장치를 확보하고 있다. 그리고 2003년안의 경우도 전체로서의 정책목표가 이러한 취지와 크게 다르지 않다고 할 수 있다.

56) 실제 인터넷실명제의 원조는 2004. 3. 12. 개정된「공직선거 및 선거부정방지법」제82조의6이었다. 여기서는 선거에 관한 게시판이용은 성명과 주민등록번호의 일치여부를 확인한 후 할 수 있도록 하였따.

57) 헌법재판소 2012. 8. 23. 선고, 2010헌마47・252(병합) 결정 [정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 제1항 제2호 등 위헌확인]

-그것이 국가감시든, 작업장 또는 소비자 감시든 관계없이-에 있어 중요한 모멘텀을 제공한다. 비록 공공기관 등의 게시판에 대한 인터넷실명제와 공직선거법상의 인터넷실명제는 여전히 그 명목을 유지하고 있기는 하지만, 그럼에도 불구하고 이 한정된 위헌선언의 의미는 적지 않다. 그것은 첫째, 질서 또는 선풍양속을 빌미로 사이버공간을 침투하는 국가적 규제의 가능성을 일부 차단하고 보다 자유로운 의사소통의 가능성을 마련하였다는 의미를 가진다. 인터넷상의 의사소통행위에 대하여 국가적 개입의 방법과 절차, 한계를 명확히 함으로써 국가로부터 자유로운 인터넷 공간을 열어두고 있는 것이다. 뿐만 아니라 둘째, 익명성의 헌법적 의미를 명확히 함으로써 그것이 소비자감시가 이루어지는 사적 영역에서도 개인정보보호를 위한 규제의 가능성을 마련한다. 이를 조망하기 위하여 우선 위의 헌법재판소 결정부터 살펴보고 그것의 의미를 다시 구성해 보기로 하자.

2. 헌법재판소의 결정

2.1. 결정요지

이 사건은 인터넷실명제를 규정한 정보통신망법이 ①인터넷게시판이용자의 익명표현의 자유와 개인정보자기결정권을 침해하며, ②인터넷언론사의 언론의 자유와 그 실명확인비용의 지출로 인한 직업수행의 자유를 침해한다는 주장에 대한 헌법적 판단을 내린 것이다. 여기서 헌법재판소는 ①게시판 이용자가 자신의 신원을 누구에게도 밝히지 아니한 채 익명으로 자신의 사상이나 견해를 표명하고 전파할 익명표현의 자유와 ②그러한 게시판 이용자의 표현의 자유에 대한 제한으로 말미암아 게시판 이용자의 자유로운 의사표현을 바탕으로 여론을 형성·전파하려는 정보통신서비스 제공자의 언론의 자유, 그리고 ③게시판 이용자가 자신의 개인정보에 대한 이용 및 보관에 관하여 스스로 결정할 권리인 개인정보자기결정권을 이 사건의 헌법적 쟁점으로 선택하였다. 하지만, 청구인들이 주장한 ④인터넷실명제가 사전검열이라는 주장과 ⑤평등권침해, ⑥사생활의 침해라는 주장은 받아들이지 않았다. ④사전검열 주장에 대하여는 "게시 글의 내용에 따라 규제를 하는 것이 아니"기 때문에 사전검열금지의 원칙에 해당되지 않는다고 보았으며, ⑤와 ⑥의 주장은 위의 ①-③의 판단으로 포섭될 수 있다고 본 것이다.

우선 헌법재판소는 입법목적의 정당성과 규제수단의 적합성은 별다른 판단 없이 인정하고 있다. 즉, 인터넷실명제는 "인터넷상의 언어폭력, 명예훼손, 불법정보의 유통 등을 방지"하고 "게시판을 보다 책임 있는 공론의 장이 되도록 유도하여 건전한 인터넷 문화를 조성하기 위한" 목적을 가진 것으로 이는 정당하다고 보았다. 그리고 이러한 목적을 달성하기 위한 수단으로 "향후 신원 확인을 통하여 형사처벌 또는 손해배상책임을 부담할 수도 있다는 점을 인식하게 하여 표현내용에 신중을 기하고 불법정보 등의 게시를 자제하도록" 하는 동시에 "실제로 피해가 발생

한 경우에는 피해자 구제를 위하여 가해자를 특정할 수 있는 기초자료를 확보”하는 것인 만큼 그 또한 적합한 것이라고 하였다.

하지만, 침해의 최소성에 있어서는 심각한 하자를 제기한다. 즉, 가해자추적은 “인터넷 주소 등의 추적 및 확인 등을 통하여서도 할 수 있다”고 하면서, 가해자가 타인의 컴퓨터 또는 아이디를 이용하는 경우와 마찬가지로 “본인확인제에 의하더라도 가해자가 주민등록번호와 명의를 도용하는 경우에는 가해자를 특정하기 어렵다”는 점을 지적하면서 가해자의 은폐시도에 대하여는 일반적인 수사기법을 통해 극복할 수 있음을 제시한다. 또한 피해자 구제의 필요성은 당해 정보의 삭제·임시조치, 불법정보 취급의 거부·정지 또는 제한명령 등이나 사후적인 손해배상 또는 형사처벌 등의 방법을 통하여 충분히 달성할 수 있다고 한다.

나아가 이 본인확인제는 목적 달성에 필요한 범위를 넘어서는 과도한 규제를 하고 있다고 보면서, “본인확인의 대상인 ‘게시판 이용자’는 ‘정보의 게시자’뿐만 아니라 ‘정보의 열람자’도 포함”하고 있다는 점에서 과잉규제이자, 동시에 인터넷 이용자 수의 산정기준이나 그 산정의 정확성이 명확하지 않음으로써 본인확인제의 적용범위를 광범위하게 정하고 이에 따라 법집행자에게 자의적인 집행의 여지를 부여하고 있다고 하였다. 그 외에도 본인확인정보를 보관하여야 하는 기간은 게시판에서 당해 정보가 삭제되지 않는 한 무기한에 이르고 있음도 과잉규제에 해당한다고 보았다.

법익의 균형성부분에 관하여는 이 제도가 “국내 인터넷 이용자들의 해외 사이트로의 도피, 국내 사업자와 해외 사업자 사이의 차별 내지 자의적 법집행의 시비로 인한 집행 곤란의 문제를 발생시키고 있”어 “당초 목적과 같은 공익을 실질적으로 달성하고 있다고 보기 어렵다”고 보았다. 뿐만 아니라 “본인확인제 이후에 명예훼손, 모욕, 비방의 정보의 게시가 표현의 자유의 사전 제한을 정당화할 정도로 의미 있게 감소하였다는 증거는 찾아볼 수 없다”는 것도 고려대상이 되었다. 이렇게 과소한 효과에 반하여 본인확인제에 의한 익명표현의 자유의 제한은 매우 중대하여, “기간 제한 없이, 표현의 내용을 불문하고 주요 인터넷 사이트의 대부분의 게시판 이용과 관련하여 본인확인을 요구하는 것”은 “정보 등을 게시하고자 하는 자가 무엇이 금지되는 표현인지 확신하기 어려운 상태에서 본인의 이름, 주민등록번호 등의 노출에 따른 규제나 처벌 등 불이익을 염려하여 표현 자체를 포기하게 만들 가능성이 높고, 인터넷을 악용하는 소수의 사람들이 존재하고 있다는 이유로 대다수 시민의 정당한 의사표현을 제한하는 것으로서 익명표현의 자유에 대한 과도한 제한”을 가하고 있다고 보았다. 뿐만 아니라, “주민등록번호를 부여받을 수 없는 외국인이나 주민등록번호가 없는 재외국민에 대하여 게시판에의 정보 게시를 봉쇄함으로써 그들의 표현의 자유를 사실상 박탈하는 결과에 이르고 있다”고 판시하였다. 아울러 “정보통신서비스 제공자에 대한 본인확인정보 보관의무 부과로 인하여 게시판 이용자의 개인정보가 외부로 유출되거나 부당하게 이용될 가능성이 증가함에 따라 게시판 이용자가 입는 불이익 및 수사기관 등이 정보통신서비스 제공자

에게 이용자의 개인정보 제출을 요청하는 경우 발생할 수 있는 본인확인정보의 보관목적외 사용 우려에 비추어 보면, 개인정보자기결정권의 제한 역시 중대함을 부인할 수 없다”는 점도 위헌판단의 이유로 제시되었다.

2.2. 평가

이 결정은 그 결정문에서도 말하고 있듯이, “국민 개인적인 차원에서는 자유로운 인격발현의 수단임과 동시에 합리적이고 건설적인 의사형성 및 진리발견의 수단이 되며, 국가와 사회적인 차원에서는 민주주의 국가와 사회의 존립과 발전에 필수불가결한 기본권이 되는” 표현의 자유를 “익명이나 가명으로 이루어지는 표현”에까지 확장하였다는 점에서 상당한 의미를 가진다. 익명·가명의 표현은 “외부의 명시적·묵시적 압력에 굴복하지 아니하고 자신의 생각과 사상을 자유롭게 표출하고 전파하여 국가권력이나 사회의 다수의견에 대한 비판을 가능하게 하며, 이를 통해 정치적·사회적 약자의 의사 역시 국가의 정책결정에 반영될 가능성을 열어 준다는 점에서 표현의 자유의 내용에서 빼놓을 수 없는 것”이라고 본 것이다.

나아가 정보통신서비스 제공자가 보관하는 개인정보는 경우에 따라서는 외부에 유출되어 부당하게 이용될 가능성도 위헌여부의 판단에 있어 중요한 고려사항임을 밝힘으로써 개인정보자기결정권에 대한 사실상의 침해가능성도 입법자의 입법형성 혹은 입법재량의 한계를 이루게 됨을 명확히 하고 있다. 입법과정에서 선택한 규율의 수단이 최소침해에 이를 것만을 요구하는 수준을 넘어, 그 수단을 선택한 결과(output과 함께 outcome이라는 의미에서) 또 다른 위험이 파생될 가능성-일종의 추상적 위험의 수준에서의 가능성-이 있는지의 여부도 고려되어야 한다고 본 것이다.

하지만 그럼에도 불구하고 이 결정은 나름의 한계를 가진다. 표현의 자유에 대한 헌법재판소의 판단이 너무 한정된 것이라서 향후의 확장성을 기대하기 어렵다는 한계도 아울러 가지고 있는 것이다. 우선 첫째, 청구인측이 주장한 사전검열원칙 위반의 문제에 대해서는 너무도 쉽게 그를 쟁점에서 제거한 것이 눈에 띈다. 헌법재판소는 “본인확인제”는 “게시 글의 내용에 따라 규제를 하는 것이 아니고”라고 하지만, 이는 어떠한 표현에 실명이나 가명을 밝히거나 혹은 익명으로 아예 이름을 밝히지 않는 것 등은 그 자체 표현의 내용을 이룬다는 점을 감안하지 못한 소치라 할 것이다. 문자 상으로는 똑같은 표현이라 하더라도 그것을 누가 말하였는가에 따라 다른 의미를 부여할 수 있다. 특히 익명표현과 현명표현은 그 표현자에 대한 신뢰의 문제를 부수함으로써 표현을 받아들이는 자가 어느 정도로 그 표현을 수용하는가를 결정하는 가장 중요한 요소 중의 하나가 된다. 그리고 바로 이런 연유에서 익명·가명으로 표현할 수 있는 자유는 표현의 자유의 중요한 부분으로 자리잡게 되는 것이다. 따라서 본인확인제는 내용에 의한 규제에 해당하며, 만약 이름을 어떻게 밝히는가에 따라 표현할 수 있거나 못하거나가 결정된다면 그것은 사전적 내용심사에 해당하여 사전검열금지의 원칙에 위반되는 것이라 판단했어야 했다.

이 점은 미국 연방대법원의 판결에서도 명확히 드러난다.[58]

유권자에게 정보를 제공하고자 하는 주의 목표(이익)가 그 문건에 표현되어 있는 논쟁들을 지지하거나 깎아내릴 수도 있는 추가적인 정보를 제공하는 것에 불과하다고 한다면, 당 법원으로서는 화자(speaker)의 신원은 작가가 포함시키든지 빼든지 마음대로 결정할 수 있는, 그 문건의 다른 부분과 전혀 다를 바 없는 것이라고 판단한다.

유권자들에게 [발화자의 신원과 같은] 추가적인 관련정보를 제공하도록 함으로써 얻어지는 단순한 주의 이익은, 작가가 생략할 수도 있는 내용을 진술하라고 하거나 공개하라고 요구하는 주의 명령을 정당화하지 못한다.

이 판결은 선거와 관련한 팜플렛이나 리플렛에 실명공개하도록 하고 위반 시에 처벌하겠다는 규정을 위헌이라고 선언한 것이다. 실명으로 팜플렛을 작성하는가 아니면 익명·가명으로 작성하는가는 작가가 결정할 수 있는 것이며 그것은 그 문건의 다른 부분을 작가가 결정할 수 있는 것과 마찬가지로 보장되어야 한다는 취지이다.

요컨대, 헌법재판소는 실명/익명/가명의 게재여부를 표현물의 다른 내용과 같은 성격의 것으로 규정하고 이 모든 것이 조합되어 하나의 표현을 이룬다고 보았어야 했다. 그리고 이런 논리에 따라 헌법재판소는 게시판실명제를 사전검열로 규정한 다음 다른 논의로 나아갈 것도 없이 위헌판단을 하는 것이 옳았다.

둘째, 청구인측이 주장한 평등원칙 위반의 점도 마찬가지로 판단했어야 하였다. 오프라인에서의 표현과 온라인에서의 표현은 그 실질에 있어서는 같습니다. 그런데도 실명제는 온라인에서만 강제하니 차별이라는 주장이 나올 수 있다. 문제는 온라인상의 표현과 오프라인상의 표현을 같이 볼 것이냐(그렇다면 실명제는 차별이다), 다르다고 볼 것이냐인데, 헌재는 이 부분의 판단을 하지 않았다. 실명제가 그 자체 위헌이면 평등이니 차별이니 할 것 없이 청구인측이 만족하지 않겠냐는 입장이었던 것이다.

그런데 실상은 그렇지 않다. 양자가 같으나 다르냐의 판단이 이루어져야 향후 대체입법이 이루어질 때 그에 대처할 수 있기 때문이다. 특히 헌재는 인터넷에서의 표현행위는 출판과 같은 맥락에서 이해되어야 한다는 판단을 내린 적이 있다.[59] 그렇다면 온/오프라인에 대한 규제는 동일한 것이어야 한다는 것인지, 아니면 그럼에도 불구하고 양자는 달리 규제할 수 있다, 그 이유는 무엇이다 라고 판단을 해 주었어야 했다. 오프라인에 비하여 온라인상의 표현은 어떻게 다르기 때문에 어떠한

58) McIntyre v. Ohio Elections Comm'n (93-986), 514 U.S. 334 (1995) "Insofar as the interest in informing the electorate means nothing more than the provision of additional information that may either buttress or undermine the argument in a document, we think the identity of the speaker is no different from other components of the document's content that the author is free to include or exclude." "The simple interest in providing voters with additional relevant information does not justify a state requirement that a writer make statements or disclosures she would otherwise omit."

59) 예컨대, 헌법재판소 2002. 6. 27. 선고 99헌마480 결정

규제의 가능성이 존재한다는 명확한 지침을 입법자와 행정부에 주었어야 했다는 말이다.

셋째, 헌재는 익명표현의 자유도 표현의 자유의 한 내용이라고 하면서도 표현의 자유에 대한규제입법의 판단기준인 명백성(명백한 위험)의 원칙을 적용하지 않았다. 헌재는 그동안 미국식의 명백하고도 현존하는 위험의 법리에서 약간 후퇴한, 명백한 위험의 법리를 사용해 왔다. 국가보안법상의 이적동조죄 한정합헌, 집시법한정합헌 등의 사건에서 "실질적 해악을 미칠 명백한 위험성이 있는 행위" "직접적인 위협을 가할 것이 명백한 경우" 등의 표현을 쓰고 있다.[60] 하지만 이 사건 결정에서는 이런 법리를 전혀 적용하지 않았다.

그것은 목적의 정당성과 수단의 적합성을 판단하는 부분에서도 전혀 고려되지 않았다. 그냥 "언어폭력, 명예훼손, 불법정도의 유통 등을 방지하기 위하여"라는 말로 넘어가 버리고 그나마도 표현자에게 '까불면 다쳐'식으로 협박하여(소위 일반예방?) 이런 목적을 추구하는 것이 적합하다고 판단하고 있다. 이는 심각한 문제가 있는 판단으로 향후 실명제가 아닌 다른 국가규제에도 그대로 적용하여 합헌선언을 할 우려가 적지 않은 것이다. 실제 이 명백한 위험의 존재는 국가가 입증하여야 할 것이나 우리 헌재는 아직도 입증책임 전환이라는 판단에까지 나아가지는 못 하고 있다. 그렇다 하더라도 최소한 '명백한 위험'에 상응할 정도로 실질적인 증명이 존재해야 하는데 헌재는 그냥 국가의 답변을 그대로 인용하면서 아무런 검증도 하지 않은 채 '그럴듯한 목적과 그럴 수도 있어 보이는 수단'을 인정해 버리고 말았다.

이 점은 나중에 법익의 균형성 부분에서도 이상한 형태로 변형되었다. 실제 명백성의 원칙은 표현에 대한 규제 그 자체의 허용성 여부를 판단하는 기준이다. 명백한 위험이 있지 않으면 규제를 하지 말아야 하는 것이지요. 그런데 헌재는 이 판단은 하지 않은 채, 위에서 말한 어중간한 목적이 있으니 규제할 수도 있다고 전제하고, 규제는 해도 되는 데 너무 심한 규제를 하였다는 선에서 판단을 그치고 만다. "표현의 자유는 민주주의의 근간이 되는 중요한 헌법적 가치이므로 표현의 자유의 사전 제한을 정당화하기 위해서는 그 제한으로 인하여 달성하려는 공익의 효과가 명백하여야 한다"는 것이 헌재의 입장이지만, 이는 종래 헌재가 가지고 있던 명백성의 법리를 뒤집는(?) 것일 수도 있다는 점에서 상당히 우려되는 서술이다. 실제 "공익의 효과가 명백하여야 한다"는 판단은 수단의 적합성에서 적용해야 할 명제이고 그 전제는 명백성의 원칙이어야 한다는 것이다.

3. 헌법재판소 결정과 본인확인

이러한 헌법재판소의 결정은 여전히 양적 한계를 가진다. 그것은 공직선거법상의

60) 예컨대, 1990. 4. 2. 선고, 89헌가113 결정; 1990. 6. 25. 선고, 90헌가11 결정; 1992. 1. 28. 선고, 89헌가8 결정 등

인터넷실명제를 무효화하지 못 하였고, 나아가 공공기관 등의 게시판실명제 또한 방치하고 있다. 실제 공직선거법상의 인터넷실명제의 경우 헌법재판소는

소수에 의한 여론 왜곡으로 선거의 평온과 공정이 위협받아 발생하는 사회경제적 손실과 부작용을 방지하고 선거의 공정성을 확보하기 위한 것이므로 목적의 정당성이 인정되고 그 수단의 적합성 또한 인정되며, 인터넷의 특성상 흑색선전이나 허위사실이 빠르게 유포되어 정보의 왜곡이 쉬운 점, 짧은 선거운동기간 중 이를 치유하기 불가능한 점, 인터넷이용자의 실명이 표출되지 않고 다만 '실명확인' 표시만이 나타나는 점을 고려하면, 피해를 최소화하기 위한 요건도 갖추었다[61]

고 하여 일반적인 인터넷실명제와는 성격이 전혀 다름을 제시한 바 있다. 즉, 국민주권주의의 실천방식으로 헌법재판소가 가장 큰 가치를 부여하고 있는 선거와 관련된 사항이며 그 중에서도 선거의 평온과 공정이라는 본질적 가치를 보호하기 위한 제도인 만큼 나름의 보호가치가 충분하며 우리 선거법제상 지나치게 짧은 선거운동기간이라는 점도 더불어 고려되었다. 따라서 이 공직선거법에 대한 위헌여부의 판단은 별론으로 하더라도 그것을 일반적인 인터넷실명제에 확장적용하는 것은 타당하지 않다 할 것이다. 즉, 이러한 헌법재판소의 결정근거를 공공기관 등의 게시판실명제에까지 확대하여 전자가 합헌이므로 후자도 합헌이다라는 식의 판단은 곤란하다는 것이다. 오히려 익명표현이 가지는 비판적 기능을 감안할 때 더더욱 익명표현의 가능성은 열어두어야 할 것이다.

그러나 이 모든 의미에도 불구하고 이 헌법재판소의 결정이 가지는 특별한 의미는 그것이 국가감시의 한계를 설정하고 있다는 점이다. 헌법재판소는 인터넷상에서 의사소통하는 자들에 대한 모니터링을 용이하게 하기 위한 수단으로서의 실명제는 허용되지 않는다고 보았다. 실명제가 아니더라도 "인터넷 주소 등의 추적 및 확인 등" 오프라인에서의 수사기법을 사용하여 그 범법행위를 사후적으로 추적, 관리할 수 있는 만큼 별도의 실명확인수단은 부가적인 규제로서 과도한 기본권제한에 해당한다고 본 것이다.

이러한 논의는 그대로 주민등록번호제도나 현재 인터넷상에서 과도하게 사용되고 있는 본인확인제에 적용할 수 있다. 국가(혹은 사인도 경우에 따라서는)가 주민등록번호와 같은 일신전속적이고 항구적인 개인식별자를 사용하거나 수집하는 것 또는 실명확인이나 본인확인에 대하여 다른 대체수단의 존재여하에 따라 그 위헌성의 여부를 달리 판단할 수 있는 여지를 마련하고 있는 것이다. 부연하자면 실명확인이나 본인확인 또는 개인식별자의 수집이 이루어지는 상황이 포털 등에서의 의사소통이나 정보열람을 목적으로 하는 경우는 의당 이런 법리가 적용되어야 할 것이며(물론 동의에 의한 제공은 별론으로 하되, 이는 후술함), 전자상거래 등의 경우에도 당사자의 정보제공동의의 범위와 한계를 결정하는 주요한 지표로 작용할 수 있다는 것이다. 이는 절을 바꾸어 살펴보자.

---

61) 헌재 2010. 2. 25. 2008헌마324

Ⅳ. 우리나라의 본인확인제

1. 본인확인제와 실명확인제

위의 헌법재판소 결정(그 심판대상인 정보통신망법 포함)에서는 “본인확인제”라는 용어를 사용한다. 하지만, 이 용어는 실명확인제라는 용어와 혼용하여 사용되고 있어 약간의 혼란을 야기한다. 대체로 인터넷상 “실명확인”은 인터넷 이용자가 사용하는 명의가 실제로 존재하는 자의 명의인지를 확인하는 것을 말한다. 반면, “본인확인”은 현재 인터넷을 이용하는 자가 실재로 존재하는 자(실명확인)이며 현재 이용자가 본인인지(즉, 현재 이용자가 그 실재자와 동일한 자인지)를 확인하는 것을 말한다. 명의의 실재성과 본인성이 결합되어 있음을 확인하는 것이 본인확인인 것이다.

여기서 가장 중요한 요소는 신분의 공적 증명이다. 국가신분증명제는 15세기 중반부터 제도화되기 시작한 것으로 국민(혹은 주민)의 통제와 치안(범인수배)의 목적을 위해 공적 주체가 신분에 관한 공적 기록(즉, 등기부)을 확보하고 그 사본 혹은 초본(즉 신분증)을 당사자에게 교부하여 소지하게끔 한 것이다.[62] 그리고 이 신분증명제도는 본인, 등기부, 증표, 사용인 등 네 가지의 요소로 구성된다. 본인은 그의 명의를 공적 주체에 등록을 하고 그 등록부에 의거하여 증표가 발행된다. 그리고 이 증표를 이용(제시 또는 소지)하는 자와 증표상의 기재내용, 그리고 등록부상의 기재내용이 서로 일치할 때 증표제시자는 본인으로 인정되는 체계를 가진다. 만일 증표내용과 등록부 내용이 서로 다르다면 그것은 위조·변조된 증표로서 무효가 된다. 증표이용자와 증표내용이 서로 다르다면 그 증표이용자의 신원은 확인되지 못한다.

하지만 이러한 구조는 대면관계를 중심으로 하는 오프라인에서 이루어지는 방식이다. 증표의 내용이 사진이든 지문이든 혹은 신체의 일정한 특징을 서술한 문구이든 신원확인을 필요로 하는 사람은 증표의 내용과 그것을 제시하는 자 사이에 일정한 일치성이 있는가를 오감을 통하여 확인하는 것으로 신원의 확인은 종료된다. 이에 신분증명제는 증표의 진실성을 확보하고, 증표내용과 소지인의 일치성여부를 판단하기 쉽게 구성하는 것 정도가 문제될 뿐이다. 증표의 위·변조 방지책과 증표기재사항의 문제(성명, 출신지, 사진, 지문, 이름, 연령, 신체특징 등)그러나 온라인의 경우에는 이러한 감각의 방식에 의한 확인 자체가 불가능하다. 그래서 주민등록번호나 공인인증서, 신용카드, 휴대폰 혹은 i-pin과 같은 방식을 사용하고, 일정한 조회시스템을 부가한다. 디지털화할 수 있는 정보를 제공받아 그것을 사전등록 받아 관리하고 있는 공적 기관에 조회하는 방식으로 그 사람의 신분을 확인하는 것이다. 그리고 바로 이 때문에 실명확인과 본인확인의 구별이 이루어질 수밖에 없다. 즉,

62) 발렌틴 그뢰브너, 김희상 역, 너는 누구냐?, 청년사, 2005, 314면 이하

인터넷 망 저 편에 있는 사람이 현재 이용하고 있는 명의가 실재인인지를 먼저 확인해야 하며 그 실재명의를 등록한 본인이 저 편에 있는 사람인지를 다시 확인하여야 하는 체제로 구성되는 것이다.

하지만, 이러한 체제에서도 상당한 문제가 있다. 이전부터 사용해 왔던 주민등록번호에 의한 신분확인의 방법은 실명확인을 위해서는 가장 유효한 방법이기는 하지만, 주민등록번호와 성명이 해킹 등에 의해 널리 유출되어 있는 상황에서는 본인확인에는 그리 적절한 것이 되지 못 한다. 이용자가 주민등록번호와 성명을 도용하거나 차용하여 사용할 수가 있기 때문이다. 더구나 2011.3. 제정된 개인정보보호법 제24조제1항은 주민등록번호를 포함하는 고유식별번호는 정보주체의 동의를 받거나 법령에서 구체적으로 고유식별번호의 처리를 요구하거나 허용하는 경우를 제외하고는 그 고유식별번호를 처리할 수 없다고 규정하고, 또 정보통신망법 제23조의2 제1항도 본인확인기관이 아닌 정보통신서비스 제공자는 법령에서 허용하거나 혹은 방송통신위원회의 고시에 의한 경우가 아니면 주민등록번호를 수집·이용할 수 없도록 함으로써 이러한 주민등록번호의 일반적 사용은 급제동이 걸리게 되었다. 주민등록번호 자체에 내재되어 있는 개인정보들과 그로 인하여 연동될 수 있는 개인정보의 보호문제로 인하여 더 이상 주민등록번호를 보편적인 개인식별자로 사용하지 못하도록 하려는 정책의지가 깔려 있는 것이다.

2. 본인확인 수단

2.1. 관련 법규정

이에 현행법은 주민등록번호를 대체할 수 있는 수단들-“주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법”(개인정보보호법 제24조제2항), “이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법”(정보통신망법 제23조의2 제2항)-을 별도로 제공하고 있다. 아래의 표[63]는 이를 정리한 것이다.

63) 이형규, “인터넷상 주민등록번호에 의한 본인확인의 문제점과 개선방안,” 한양법학 제23권 제1집, 2012, 341-371면, 357-362면에서 정리.

법령명	조항	수집대상
개인정보보호법	24①	고유식별정보 수집금지
	24②	대체수단 제공
정보통신망법	23-2①	주민등록번호수집금지
	23-2②	대체수단 제공
전자상거래소비자보호법	6②	거래기록관련 개인정보(주민등록번호) 보존
	21①vi다	도용방지목적 실명확인(주민등록번호)
전자서명법	15①	공인인증서발급시 주민등록번호 요구가능
신용정보의 이용 및 보호에 관한 법률	24	안행부장관에 대한 주민등록번호 제공요청권
전자금융거래법	6①	주민등록번호 요청
여신전문금융업법	19②	신용카드소유자의 주민등록번호
청소년보호법	17①	연령확인용 주민등록번호 요구
공직선거법	82-⑥	인터넷실명제

2.2. 본인확인, 대체수단의 발급 및 이용실태

개인정보보호법 및 정보통신망법에 의하여 주민등록번호를 대체하는 수단으로 현재 주로 는 것은 2006. 6. 도입된 i-PIN(2009.7. i-PIN 2.0 개정)과 휴대폰, 그리고 공인인증서 등 세 가지가 있다. i-PIN은 개인정보보호법 및 정보통신망법에 의하여 방송통신위원회가 본인확인기관으로 지정한 민간기관(현재는 3개) 및 공공i-PIN센터가 발급하는 것으로 ID와 비밀번호를 입력하는 방식으로 본인확인을 하게 된다. 공인인증서에 의한 본인확인방법은 전자정부법, 전자서명법 등에 따라 현재 5개의 공인인증기관에서 발급하는 것으로 인증서 버전, 인증서 일련번호, 인증서 유효 기간, 발급기관 이름, 가입자의 전자서명 검증정보, 가입자 이름 및 신원 확인정보, 전자서명 방식 등이 포함되어 있고 사용할 때 비밀키를 암호화한 패스워드를 입력하면 자동으로 전자서명이 생성되는 방식으로 작동한다. 휴대폰의 경우에도 전기통신사업법 및 전자상거래 등에서의 소비자보호에 관한 법률 등에 의해 성명, 휴대폰번호, 이동통신사를 입력하여 확인하는 방법을 취한다. 그 외 여신전문금융업법에 의한 신용카드 방식의 본인확인방법 등이 있다. 아래의 표는 이를 정리한 것이다.

대체수단	발급기관	발급현황(누적)		
		2011년	2012년	2013년
아이핀	나이스신용평가정보	1,802,513	2,837,954	4,744,583
	서울신용평가정보	1,465,987	2,121,405	3,150,028
	코리아크레딧뷰로	139,810	296,258	825,754
	안전행정부	1,119,780	1,753,060	2,267,317
	합계	4,528,090	7,008,677	10,987,682
휴대폰 (불명확)	SKT	26,552,716	26,961,045	27,046,666
	KT	16,563,158	16,501,639	16,420,628
	LGU+	9,390,919	10,161,743	10,420,562
	합계	52,506,793	53,624,427	53,887,856
공인인증서	범용	3,076,520	3,170,079	3,204,268
	민간	26,548,700	28,381,968	29,827,199
	합계	29,625,220	31,552,047	33,031,467

※ 공인인증기관: 한국정보인증(주), (주)코스콤, 금융결제원, 한국전자인증(주), (주)한국무역정보통신

여기서 특기할 만한 것은 주민등록번호를 대체하기 위해 특별히 고안된 i-PIN의 경우 그 발급량이 다른 대체수단에 비해 현저하게 적다는 점이다. i-PIN은 주민등록번호와 달리 웹사이트에 저장되지도 않으며 폐지나 변경이 손쉽게 이루어진다는 점에서 개인정보보안성이 훨씬 뛰어난 편이다. 실제 처음 만들어진 i-PIN은 연동이 불가능하게 되어 있는 등 그 사용효용이 현저하게 낮아 보급률이 떨어질 수밖에 없었으나, 이를 개선한 i-PIN 2.0의 경우에도 교육기관 등에 의한 발급유도행위에 힘입어 약 1천만건 정도의 기록을 이룰 수 있었다.

또한 공인인증서의 경우에는 공인인증기관 외에 등록대행기관과 중계서비스기관이라는 매개기구를 설정하여 다단계의 인증절차를 밟도록 하고 있는 것이 특징적이다. 물론 이런 매개기구에 대하여는 전자서명법 등 법률적 근거는 전혀 없으며, 단지 전자서명법 제8조가 미래창조과학부장관에게 고시의 형식으로 위임한 것에 의거하여 제정된 전자서명인증업무지침(미래창조과학부고시 제2013-53호, 2013.8.8., 일부개정]만 그 근거규정으로 존재하고 있을 뿐이다. 하지만 이 전자서명법 제8조는 공인인증업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증업무수행에 있어 지켜야 할 구체적인 사항을 규정하게끔 한 것에 불과하며 등록대행이나 중계서비스라는 새로운 인증의 방식 및 절차를 규정할 수 있는 근거규정은 되지 못한다는 점에서 후술하는 바와 같이 법제적인 하자가 있는 것이라 할 수 있다.

공인인증기관 (5개)	+	등록대행기관 (626개)	+	중계서비스기관 (금융결제원, 1개)

이를 다시 이용자들에게 본인확인을 요구하는 온라인 사이트를 중심으로 구분해 보면 다음의 표와 같다.

분야	사이트	인증수단	인증업체(아이핀/휴대폰)
포털(3)	네이버	휴대폰, 유선전화, 이메일	× / NICE신용평가·서울신용
	다음	휴대폰, 유선전화, 이메일	× / 서울신용평가
	네이트	휴대폰, 이메일	× / NICE신용평가·서울신용
쇼핑몰(5)	Gmarket	아이핀, 휴대폰	NICE신용평가 / NICE신용평가
	옥션	아이핀, 휴대폰	NICE신용평가 / NICE신용평가
	11번가	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	인터파크	아이핀, 휴대폰	서울신용평가 / 모바일인증
	이마트몰	아이핀, 휴대폰	서울신용평가 / 서울신용평가
홈쇼핑(3)	CJ오쇼핑	아이핀, 휴대폰	서울신용평가 / NICE신용평가
	GS홈쇼핑	아이핀, 휴대폰	서울신용평가 / 모바일인증
	현대홈쇼핑	아이핀, 휴대폰, 공인인증서	서울신용평가 / 드림시큐리티
인터넷서점 (3)	교보문고	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	예스24	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	알리딘	아이핀, 휴대폰	서울신용평가 / 모바일인증
쇼설커먼스 (3)	쿠팡	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	티켓몬스터	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	위메프	아이핀, 휴대폰	서울신용평가 / 모바일인증
통신(3)	SKT	아이핀, 휴대폰	NICE신용평가 / ?
	KT	아이핀, 휴대폰	서울신용평가 / 모바일인증
	LGU+	아이핀, 휴대폰	NICE신용평가 / 모바일인증

분야	사이트	인증수단	인증업체(아이핀/휴대폰)
신문(5)	조선일보	아이핀	서울신용평가 / ×
	중앙일보	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	동아일보	아이핀, 휴대폰	NICE신용평가 / 모바일인증
	한겨레신문	아이핀	NICE신용평가 / ×
	경향신문	아이핀, 휴대폰	코리아크레딧 / 코리아크레딧
방송(3)	KBS	아이핀, 휴대폰	NICE신용평가 / 드림시큐리티
	MBC	아이핀, 휴대폰	서울신용평가 / 모바일인증
	SBS	아이핀, 휴대폰	NICE신용평가 / NICE신용평가
게임(3)	넥슨	아이핀, 휴대폰, 이메일	NICE신용평가 / 모바일인증
	네오위즈	아이핀, 휴대폰, 이메일	서울신용평가 / 모바일인증
	엔씨소프트	아이핀, 휴대폰, 이메일	서울신용평가 / 모바일인증
기타(3)	CGV	아이핀, 휴대폰	NICE신용평가 / NICE신용평가
	멜론	아이핀, 휴대폰	NICE신용평가 / NICE신용평가
	잡코리아	아이핀, 휴대폰	NICE신용평가 / 모바일인증

3. 현행 본인확인 수단의 문제점

3.1. 주민등록번호제도로의 회귀

우리나라에서 그동안 본인확인의 가장 주요한 수단으로 사용되어 왔던 것은 주민등록증이며, 온라인상에서는 그에 기재된 주민등록번호와 주민등록증발급일자 등이었다. 하지만, 이러한 주민등록번호가 가지는 문제점-특히 해킹 등에 의한 도용・차용의 가능성-으로 인하여 개인정보보호법이나 정보통신망법에서는 원칙적으로 이의 수집・사용을 금지하였다. 그리고 그 대체수단으로 i-PIN이나 공인인증서, 휴대폰, 신용카드 등을 사용하도록 하였다. 하지만, 그럼에도 불구하고 이 제도들은 하나같이 주민등록번호로 귀일한다는 점에서 그 효율성은 물론 효과성조차 신뢰하기 어렵게 된다.

i-PIN의 경우 그것을 발급받기 위해서는 휴대폰인증, 신용카드인증, 범용공인인증서인증, 혹은 대면확인(방문하여 신분증 제시) 등의 본인확인이 선행되어야 한다. 하지만 후술하듯 이러한 선행본인확인제도 역시 주민등록번호가 기반이 되어 구축된 것들이다. 신용카드의 경우에는 금융정보수집과정에서 주민등록번호가 수집되며, 공인인증서의 경우에도 신분증 사본의 제출이 요구되며 성명, 주민등록번호, 주소, 전

화번호 등의 정보가 수집된다.

휴대폰은 그 대표적인 경우로서 현재 휴대폰인증기관으로 되어 있는 3사 모두 휴대폰 가입시에 주민등록번호를 제출할 것을 요구하고 있다. 물론 이들은 정보통신망법 제23조의2 제1항 제3호에 따라 “영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우”에 해당하기 때문에 주민등록번호를 수집할 수 있다고 주장할 수 있을 것이나, 휴대폰 가입자의 경우에도 휴대폰을 단순한 통화의 목적으로만 사용하되 본인확인의 수단으로 하지 않으려는 의지를 가진 이용자에 대해서도 대체수단을 마련하지 않은 채 주민등록번호를 수집하는 관행은 이해하기 어렵다. 즉, 대부분의 통신사들이 주민번호를 수집, 이용하는 목적으로 제시하는 사항들 중 “이동전화서비스의 가입고객을 대상으로 한 본인확인서비스 제공”이라는 항목을 제외한 나머지 항목들(온라인신청서 작성을 위한 본인확인/인증, 서비스가입/변경/해지 처리 등, 계약의 이행에 필요한 업무의 위탁 등)은 대체수단에 의한 본인확인으로써 충분히 처리할 수 있는 것이기 때문이다.

결국 모든 본인확인 대체수단의 출발점은 주민등록번호에 귀결된다. 이는 제도설계에 있어 중대한 하자를 의미한다. 정보통신망법 제23조의3 등에서 본인확인기관을 지정하고 대체수단의 개발·제공·관리업무를 수행하도록 한 제도의 취지는 모두 같은 법 제23조의2 제1항에서 “주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법”을 “대체수단”으로 규정함으로써 가능했던 것이다. 즉, 본인확인을 위한 대체수단에는 주민등록번호가 전제되어 있지 않아야 양자는 서로 “대체” 가능한 것이 된다.[64] 하지만, 현재의 체제는 본인확인의 대체수단이 아니라 주민등록번호의 또 다른 변형에 불과한 것이 되어 있다.

그리고 이 과정에서 통일식별자로서의 주민등록번호가 가지는 무한연동가능성이라는 폐해가 그대로 잔존하게 되는 문제를 낳게 된다. 실제 i-PIN 2.0의 가장 큰 특징으로 제시되는 것중의 하나가 기업에서 이 i-PIN을 가지고 복수의 데이터베이스를 연동할 수 있도록 하였다는 점이다. 나아가 본인확인기관의 지정 등에 관한 기준 별표2의 7-5는 본인확인기관 간 상호연동(나목), 공공부문 시스템과의 연동(라목), 중복가입확인정보의 제공(마목), 연계정보의 제공(바목) 등 다양한 연동장치에 관한 규정들을 설정하여 본인확인기관의 지정요건으로 삼고 있다. 이는 본인확인이라는 정보수집의 목적 외에 다른 부가가치의 증식에 개인정보를 사용하는 것이 되어 개인정보보호의 원칙에 반하는 셈이 된다. 물론 이 과정에 이용자의 동의를 구하는 절차를 경유하겠지만, 이렇게 다양한 정보의 연동까지 요건으로 삼아 본인확인기관의 시설로 충당하게 만들어놓고 이를 바탕으로 다시 이용자에게 굳이 그 정보연동의 동의를 구하는 것 자체가 본말이 전도된 것이라는 느낌을 피할 수 없다. 더구나 몇 개 되지 않

64) 본인확인기관 지정 등에 관한 기준[방송통신위원회고시 제2012-48호, 2012.8.8, 제정] 별표2의 7-5, 라목에서는 본인확인기관은 “공공부문 인터넷 사이트에서 본인확인정보 사용 시 해당 본인확인정보를 주민등록번호로 변환하여 한국인터넷진흥원에 전송하는 기능”을 갖출 것을 요구하고 있음은 이의 단적인 예가 된다.

은 본인확인기관 모두에 대해 고시의 형태로 연동이 강제되어 있는 현실에서는 이용자가 이러한 동의를 거부할 방법도 없다. 요컨대, 본인확인기관의 본래 기능은 본인확인에 있는 만큼 그 기능에만 한정하여 업무를 처리하도록 하는 것이 개인정보보호라는 점뿐 아니라 기본권의 최대보장이라는 헌법이념에도 적합한 방식이다.

3.2. 본인확인의 강박증: 불확실성에 수반되는 위험비용의 전가

본인확인제도의 또 다른 문제점은 지나치게 많은 본인확인수요가 발생하고 있다는 점이다. 다음 표는 우리나라의 주요 포털 및 사이트에서 본인인증을 요구하는 방식을 조사, 정리한 것이다. 일견하여 특징적인 것은 모든 사이트가 본인인증을 요구하고 있고 그것도 결제시나 성인인증 시에 다시 한번 더 본인 인증할 것을 요구하는 경우가 적지 않다는 점이다. 특히 헌법재판소의 결정 이후 민간부문에서의 인터넷실명제는 폐지되었음에도 불구하고 이들 사이트는 여전히 실명확인 혹은 본인확인의 단계에까지 나아가고 있다. 예전과 다름없이 이들 사이트들은 이용자들의 익명표현의 자유를 보장하지 않고 있는 것이다.

물론 이러한 본인인증 강박증은 여러 가지의 장점을 가져다준다. 짐작컨대, 중복가입을 방지하며 아이디/패스워드를 망각하였을 경우 인증정보를 활용해 쉽게 복구할 수 있다는 장점도 있을 것이다. 하지만, 그보다 더 큰 이유는 인터넷상에서 발생할 수 있는 명예훼손이나 모욕, 타인의 권리침해 등의 위험이 발생할 때를 대비하여 손쉽게 가해자를 추적하고 처벌할 수 있게 하는 것 또는 그러한 가능성을 공시함으로써 일반예방의 효과를 거두고자 하는 것에 있다 할 것이다. 아울러 이러한 인터넷상의 질서유지의 의무를 지는 국가의 입장에서는 이 사이트들의 자료제출 협조만으로도 범법자를 발견하고 처단할 수 있을 뿐 아니라, 어느 정도의 자기검열의 효과도 거둘 수 있다는 점에서 상호 공생의 관계에 놓이게 된다. 한 마디로, 인터넷 사이트를 개설함으로써 필연적으로 발생하게 되는 일정한 위험을 사이트 개설자나 국가가 부담하지 않고 본인확인의 방식을 통해 사이트 이용자에게 전가하는, 그래서 개인정보를 노출하게 만들고 자기검열에 빠지게 하는 방식을 사용하고 있는 것이다.

문제는 이러한 본인인증제의 남용에도 불구하고 국가는 이에 대해 별다른 규제를 하지 않고 있다는 점이다. 앞서 설명한 헌법재판소의 결정에서 보듯 인터넷 공간에서의 의사소통은 최대한 보장되어야 하는 헌법상의 최고가치중의 하나이다. 그리고 본인확인제도는 익명으로 표현할 수 있는 자유에 대한 중대한 침해가 된다. 물론 이는 국가와의 관계 속에서 충분한 의미를 발휘할 것이나, 기본권의 객관성을 고려한다면 국가는 그 실현을 위해 최대한 노력해야 할 의무를 지게 된다. 즉, 이러한 본인인증의 남발을 막기 위한 입법적 조치를 하여야 한다는 것이다. 하지만 현재의 정보통신망법이나 개인정보보호법은 주민등록번호의 수집만 원칙적으로 금지하고 있을 뿐이지 본인확인에 관하여는 별다른 제재규정을 두지 않고 있어 그 주민등록번호를 기반으로 구성되는 대체수단의 수집에 대해서는 오히려 권장하는 듯한 뉘앙스까지 주고 있는 실정이다.

사이트명	회원가입	게시글, 댓글	유료 결제	성인인증	기타 콘텐츠 이용
네이버	본인인증	회원 로그인	회원 로그인 후 본인인증	회원 로그인 후 본인인증	회원 로그인
다음	본인인증	회원 로그인	회원 로그인 후 본인인증	회원 로그인 후 본인인증	회원 로그인
네이트	본인인증	회원 로그인	회원 로그인 후 본인인증	회원 로그인 후 본인인증	회원 로그인
조선일보	본인인증	회원 로그인	회원 로그인	-	회원 로그인
중앙일보	본인인증	회원 로그인 소셜 로그인	회원 로그인	-	회원 로그인
동아일보	본인인증	회원 로그인 소셜 로그인	회원 로그인	-	회원 로그인
한겨레신문	본인인증	회원 로그인 소셜 로그인	회원 로그인	-	회원 로그인
경향신문	본인인증	회원 로그인 소셜 로그인	회원 로그인	-	회원 로그인
Gmarket	본인인증	회원 로그인	회원 로그인 비회원 본인확인	로그인 후 본인인증 (비회원 휴대폰 인증)	로그인 불필요
옥션	본인인증	회원 로그인	회원 로그인 비회원 본인확인	로그인 후 본인인증 (비회원 휴대폰 인증)	로그인 불필요
11번가	본인인증	회원 로그인 소셜 로그인	회원 로그인 비회원 본인확인	로그인 후 본인인증 (비회원 이용 불가)	로그인 불필요
인터파크	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	로그인 후 본인인증 (비회원 이용 불가)	로그인 불필요

사이트명	회원가입	게시글, 댓글	유료 결제	성인인증	기타 콘텐츠 이용
이마트몰	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	로그인 후 본인인증 (비회원 이용 불가)	로그인 불필요
CJ 오쇼핑	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	로그인 후 본인인증 (비회원 휴대폰 인증)	로그인 불필요
GS 홈쇼핑	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	로그인 후 본인인증 (비회원 휴대폰 인증)	로그인 불필요
현대홈쇼핑	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	회원 로그인 (비회원 이용 불가)	로그인 불필요
KBS	본인인증	회원 로그인	회원 로그인	회원 로그인	로그인 불필요
SBS	본인인증	회원 로그인	회원 로그인	회원 로그인	로그인 불필요
MBC	본인인증	회원 로그인	회원 로그인	회원 로그인	로그인 불필요
SKT	본인인증	회원 로그인	회원 로그인	-	로그인 불필요
KT	본인인증	회원 로그인	회원 로그인 (비회원 휴대폰 인증)	-	로그인 불필요
LGU+	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	-	로그인 불필요
넥슨	본인인증	회원 로그인	회원 로그인 후 본인인증	회원 로그인 후 본인인증	비로그인
네오위즈	본인인증	회원 로그인	회원 로그인 후 본인인증	회원 로그인 후 본인인증	비로그인
엔씨소프트	본인인증	회원 로그인	회원 로그인 후 본인인증	회원 로그인 후 본인인증	비로그인
교보문고	본인인증	회원 로그인 소셜 로그인	회원 로그인 (비회원 결제정보 수집)	회원 로그인 후 본인인증 (비회원 이용 불가)	비로그인

사이트명	회원가입	게시글, 댓글	유료 결제	성인인증	기타 콘텐츠 이용
예스24	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	회원 로그인 (비회원 이용 불가)	비로그인
알라딘	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	회원 로그인 (비회원 이용 불가)	비로그인
쿠팡	본인인증	회원 로그인	회원 로그인 (비회원 이용 불가)	별도인증 없음	회원 로그인
티켓몬스터	본인인증	회원 로그인	회원 로그인 (비회원 이용 불가)	로그인 후 본인인증 (비회원 이용 불가)	회원 로그인
위메프	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	로그인 후 본인인증 (비회원 이용 불가)	회원 로그인
CGV	본인인증	회원 로그인	회원 로그인 (비회원 결제정보 수집)	회원 로그인 (비회원 이용 불가)	비로그인
멜론	본인인증	회원 로그인	회원 로그인 후 본인인증 (비회원 이용 불가)	회원 로그인 (비회원 이용 불가)	비로그인
잡코리아	본인인증 이메일 인증	회원 로그인	회원 로그인 (비회원 이용 불가)	별도인증 없음	비로그인

3.3. 본인확인기관에 대한 법적 근거의 문제

전술하였듯이 공인인증서발급의 경우에는 공인인증기관 외에도 등록대행기관 및 중계서비스기관이라는 매개체가 존재한다. 문제는 개인식별정보를 수집할 수 있는 권한이 법적으로 보장되어 있는 공인인증기관이 사적인 계약을 통하여 아무런 법률적 근거도 없는 등록대행기관에 그 권한의 전부/일부를 위임할 수 있는가이다. 미래부의 답변은 “공인인증기관과 등록대행기관 두 기관간의 업무 위탁에 관한 계약은 사적 계약사항”이며 “두 기관 간 업무위탁 계약사항으로 인해 공인인증서 발급의 신뢰성이 저해되지 않도록 ‘전자서명인증업무지침’에 ‘등록대행기관’에 대해 정의하고 있음”을 강조한다. 하지만, 공인인증기관이 법률에 의하여 부여받은 주민

등록번호 수집권한을 사적 계약에 의하여 위임할 수는 없는 일이다. 공인인증기관은 비록 그 존재형식은 사적 기업 - 사인의 모습을 하고 있으나 공인인증이라는 국가신분확인의 기능을 대행하는 공적 업무를 수행하고 있다고 보아야 하며, 이러한 공적 기능의 위임은 법령의 근거가 있을 때에야 가능한 것이라 할 것이기 때문이다.

나아가 주민등록번호의 수집은 일종의 일반법적 지위를 가지는 개인정보보호법이나 정보통신망법 등에서 원칙적으로 금지하고 있다는 점을 감안할 필요가 있다. 물론 공인인증제도는 이들 법률들과는 별개의 전자서명법에 의하여 규정되고 있는 것으로 그 독자성을 인정할 수는 있을 것이나 이 경우에도 앞서 설명한 헌법재판소의 최소침해의 원칙에 충실하는 것이 바람직하다. 그 주민등록번호의 수집은 최소한에 그쳐야 하며 여기서 말하는 "최소한"이라는 개념 속에는 기관의 최소한이라는 개념도 포함된다고 보는 것이 헌법지향에 합치되는 해석이기 때문이다.

여기서 미래부가 언급하는 "전자서명인증업무지침"은 등록대행기관의 지정에 관한 사항을 규정할 수 없다고 보아야 한다. 왜냐하면 그 근거조항인 전자서명법 제8조는 "미래창조과학부장관은 인증업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증업무수행에 있어 지키어야 할 구체적 사항을 전자서명인증업무지침으로 정하여 고시할 수 있다"고 하기 때문이다. 즉, 이 전자서명인증업무지침의 내용에는 "인증업무의 안전성과 신뢰성 확보"에 관한 사항이 들어가야 하며 그 의무의 주체로 "공인인증기관"만이 규정되어 있기 때문이다. 더구나 이 "지침"은 행정규칙의 형식을 띠고 있는 만큼 공적 기능의 위임과 같은 법규사항은 가능한 한 축소하는 것이 입법위임의 법리에 적합하다고 할 수 있을 것이다.[65]

아울러 정보통신망법 제25조 제1항에 의하여 정보통신서비스 제공자가 제3자에게 개인정보의 취급을 위탁하는 경우에도 그 위탁가능한 개인정보에는 제23조의2에서 규정한 주민등록번호는 제외된다고 보아야 할 것이다. 왜냐하면 제23조의2는 일종의 특별법적 규정으로 모든 개인정보 중에서 주민등록번호의 경우에만 적용되는 특례를 규정하고 있는 것이라 보아야 할 것이며, 이러한 특례는 개인정보의 취급위탁의 경우에까지 적용되는 것이라고 보아야 할 것이기 때문이다. 즉 개인정보 중에서도 주민등록번호만큼은 일정한 조건을 충족한 정보통신서비스 제공자 "만"이 수집·이용할 수 있게 한 제23조의2의 규정취지에 비추어 그러한 정보통신서비스 제공자 아닌 자는 위탁이든 다른 방법이든 어떠한 경우에도 주민등록번호의 수집을 할 수 없다고 해야 한다는 것이다.[66]

---

65) 이에 대하여 위탁을 금지하는 규정이 없으니까 위탁 가능하다는 취지의 방송통신위원회의 답변은 이런 법리의 범주를 일탈한 것이 된다.

66) 더구나 이러한 등록대행기관에 대한 공인인증기관의 관리현황에 대한 미래부의 감독조차 제대로 이루어지지 않고 있는 듯한 현실에 미루어볼 때 이런 위탁방식의 업무처리현상이 조속히 수정되어야 할 것이다.

Ⅴ. 결론

이상에서 우리나라에서의 본인확인제도의 현실과 그 문제점을 살펴보았다. 그것은 한 마디로 그동안 시민사회에서 지속적인 비판을 받아왔던 주민등록번호제도를 외형만 변경시킨 것에 지나지 않는다. 오히려 인터넷실명제에 대한 위헌결정에도 불구하고 변형된 형태의 인터넷실명제를 강화하고 그를 통해 국가감시가 보다 치밀하게 이루어질 수 있게끔 하는 또 다른 형태의 통로가 되어 있을 뿐이다. 정보통신서비스제공자는 또 그대로 사이버공간에서 발생할 수 있는 갖가지의 위험을 회피하거나 전가할 수 있는 수단으로 그 본인확인제도를 무차별적으로 사용하고 있다. 어쩌면 국가의 감시욕구와 기업의 비용경감욕구 그리고 일부 본인인증기관들의 상업적 욕구가 결합하여 정보통신서비스의 이용자들의 개인정보를 침탈하는 거대한 구조가 형성된 것처럼 보이기도 한다.

물론 그 대안은 쉽지 않다. 헌법재판소의 결정에서도 언급하였듯이 인터넷상의 질서유지는 나름 중차대한 국가목적이며 이를 위해 국가는 적지 않게 노력해야 하는 것도 사실이다. 하지만, 그럼에도 불구하고 우리의 실태는 본인확인의 필요성에 대한 성찰은 전혀 없이 거의 무조건적으로 본인확인을 요구하고 있는 상황이다. 남용되고 오용됨으로써 정보통신서비스 이용자들만 고통을 받는 체제로 운영되고 있는 것이다. 그래서 이 문제의 극복을 위한 최선의 대책은 이 본인확인제 자체를 원점에서부터 재검토하는 일이다. 왜 주민등록제도를 기반으로 하는 국가감시체제와 직접 결합한 본인확인제도를 구성하고 여기에 모든 사이트들이 포섭되어 있는지를 다시 한 번 생각해 보아야 한다는 것이다. 뿐만 아니라 너무도 당연한 것으로 전제되어 있는 대체수단을 통한 데이터베이스의 연동이라는 구조는 개인정보보호라는 점에서 뿐 아니라 국가권력(혹은 상업권력)의 통제라는 점에서도 조속히 해소되어야 할 것이다.

실제 정보화의 문제는 헌법에서 정하는 사생활의 비밀과 같은 자기정보통제권의 문제에 그치지 않는다. 자기정보결정권의 경우는 단순히 국가가 장악하고 있거나 장악하고자 하는 정보에 대한 국민의 접근 및 관리·통제의 권리를 의미한다. 즉, 자신이 원하는 형태와 종류의 정보만을 국가가 활용할 수 있도록 하는 권리이다. 하지만, 정보화사회에 있어서의 국가의 정보권력은 이러한 국민의사에 반하는 정보확보 및 활용의 수준을 넘어선다. 그것은 국가를 고도로 집중되고 강화된 권력체로 전환시킴으로써 제한국가(limited government)의 원리에 입각하고 있는 자유민주주의의 기본질서 그 자체를 위협하는 중대한 상황을 예정하고 있다. 그 판옵티콘은 권력, 즉 사회를 지배하는 규율(discipline)이 단순히 위반자를 사회적으로 격리시키는 수준을 넘어선다. 그것은 모든 인간의 내면에 작용하여 그들이 항시적으로 감시당하고 있다는 의식을 잠재화시킴으로써 현실적인 감시와는 관계없이 권력에 의하여 설정된 행위준칙을 준수하게 되는 인간 즉, 규율된 인간을 만들어낸다. 그래서

이 판옵티콘은, 모든 인간에 대하여 그들의 의식과 생활관계까지도 지배하는, 권력의 효과를 가장 세부적이고 깊숙한 곳까지 확장시키는 “판옵티시즘(panopticism)”의 메카니즘 혹은 초감시국가(super-surveillance state)를 구축하게 되는 것이다.

여기서 본인확인제가 만연하고 있는 우리의 현실은 사적 영역 혹은 시민사회의 영역까지도 이 초감시국가에 포획되어 있는 상황을 만들어낸다. 그 본인확인제도는 정보통신서비스 제공자의 이용자에 대한 감시를 단순한 소비자감시의 수준을 넘어서서 국가감시의 수준으로까지 연동시키고 있음을 의미한다. 거의 모든 국민들이 휴대폰을 소지하고 그를 통해 의사소통하는 상황에서 본인확인이 필수적인 휴대폰은 어느 누구도 익명의 통신을 할 수 없도록 만든다. 거의 모든 포털사이트와 언론매체들이 주민등록번호가 전제되어 있는 본인확인시스템을 강요함으로써 사이버공간에서도 익명의 댓글을 달 수 있는 여지는 없어지게 된다. 경우에 따라서는 수사기관의 포털에 대한 협조요청 하나로 수많은 개인정보와 그의 통신내역들이 국가의 수중에 장악되는 것이 현실이기도 하다. 그리고 이 과정에서 권위주의 군사정권에 의해 만들어진 주민등록번호의 위력이 되살아나는 동시에 어렵게 확보한 인터넷실명제에 대한 위헌결정마저도 무위로 돌려버리고 마는 상황이 이루어지게 되는 것이다.

그리고 이 과정에서 국가는 국민들의 모든 생활관계에 관한 정보를 확보하고, 그것을 자신의 의지에 부합하도록 처리, 분석하며, 끊임없는 정보활동-감시활동을 통하여 정보를 재생산할 수 있게 된다. 나아가 모든 국민들이 의식적으로 또는 무의식적으로 국가의지에 합치되는 방향으로 자신의 생활세계를 구축해 나가도록 유도하는, 절대적인 권력을 가진 국가로 존재할 수 있게 된다.

주민등록제도에 대하여 개인정보자기결정권을 주장하는 것은 이 점에서 기본권의 실현이라는 명제에 그치지 않고 민주적 헌정질서의 확립이라는 또 다른 의미를 가진다. 그것은 개인정보에 대한 사적 이익의 향유행위를 넘어서서 초감시국가가 행사하는 절대권력을 해체하는 시민정치의 표현이기 때문이다. 우리나라의 주민등록제도-특히 주민등록번호제도는 이런 초감시국가의 등장을 예고하는 단초를 이룬다. 그것은 모든 국민으로 하여금 그의 신분 및 관련정보를 등록하게끔 강제하고 주민등록번호라고 하는 단일식별자를 통해 그 국민들의 일거수일투족을 감시할 수 있도록 만든다. 나아가 전자주민증에 대한 행정안전부의 맹목적 아집은 이런 국가적 감시의 가능성을 더욱 확장할 뿐 아니라, 그 전자칩에 접근할 수 있는 모든 사적 권력조차도 이런 초감시의 권능을 행사할 수 있도록 한다. 결국 현재의 주민등록제를 바탕으로 하는 국가신분증명제는 가장 악한 극단에서는 헌법에서 보장하고 있는 민주주의와 인간의 존엄 및 가치의 보장이라는 궁극적 이념 자체에 대한 도전이자 동시에 인간성의 본질에까지 일관체계로 통제할 수 있는 최첨단의 국가주의를 형성할 가능성을 내포하고 있다고도 할 것이다.

우리의 87년 체제는 군사적・관료적 권위주의가 행사하였던 탈정치화와 배제의 정치에 대한 시민들의 거부로부터 시작되었다. 정치영역에 대한 능동적 참여와 스

스로 정치주체로서 자각하고 인식하는 반성으로부터 현재의 민주화체제가 구성될 수 있었던 것이다. 마찬가지로 국가감시가 만들어내는 초국가의 현상 내지는 초감시사회의 형성은 이제 개인정보자기결정권으로부터 정보주권을 추출하기 시작하는 또 다른 시민들에 의해 해체될 수 있다. 그리고 바로 이 점에서 주민등록제도를 둘러싼 헌법판단은 C. Schmitt가 말하는 새로운 정치적 투쟁의 경로에 접어들게 된다. 정보사회에서의 그것은 이제 '정치적인 것'으로서의 실체를 갖추어가고 있는 것이다.

제2주제

일본에서의 사회보장 · 조세번호 제도가 프라이버시 보호에 미치는 영향

The Influence of the Social Security and Tax Number System on Privacy in Japan

Junichiro Makita*

Overview

Ⅰ. Outline of the Social Security and Tax Number System.[1)]

The government is planning to introduce the Social Security and Tax Number System (“the number system”) in 2016. This will influence a lot on privacy in Japan. I will explain this number system first.

1. Purposes

The government explains that it will adopt the number system in order to (1) enhance the social security to people who truly need it, (2) achieve the fairness of burdens such as the payment for income tax, and (3) develop the efficiency in administration.

2. The Mechanisms of the Number System

The number system has following three mechanisms.

* 하라고 법률사무소 변호사, 일본

1) See materials in English available at http://www.cas.go.jp/jp/seisaku/bangoseido/english.html

2.1. Number Assignment

The government will assign new numbers associated with up-to-date data on four types of basic information (name, address, sex and date of birth). The function of the numbers is to grasp information regarding incomes and so on and use efficiently that information for social security and taxation.

Numbers in the number system have the following five characteristics.

(i) Each and every person is assigned one Number

(ii) Each person has a unique Number

(iii) Numbers can be used in the private and public sectors

(For example, if Company A pays wages to Individual B, in order for the national and local governments to obtain a grasp of Individual B's wages, Company A must send a payment record including Individual B's number to the governments. So, Individual B must present his or her number to Company A. In that sense, the number is used from Individual B (private sector) to Company A (private sector) to the national and local governments (public sector))

(iv) Numbers shall be confirmed visually (It is necessary for Company A to confirm the number presented by Individual B)

(v) Numbers shall be associated with four types of up-to-date information

2.2. Information Sharing

Multiple institutions will share information relating to an individual by associating number system numbers and other numbers (We already have many other number systems such as the pension number system) with him or her.

In information sharing, when an institution with a database requires specific information from a database held by another institution, it uses some form of identifier (This is not number system number. Identifier is made from the number system number and the Juki Net residency registry system number) to specify the individual in question and then obtains new information.

Institutions must use an information sharing infrastructure in order to clarify the type of personal information being shared and the reason for sharing it.

2.3. Identification

The government will distribute IC cards to the public. The surface of the cards

will display the four types of basic information and a facial photograph. The IC cards also have IC chips to record numbers. The IC cards could be used for in-person identification and online authentication.

3. Extent of Procedures Including Notification and Use of the Numbers

The following is the extent of procedures in various fields in which the public will provide and use the numbers.

3.1. Pensions

Procedures related to notifications, benefit payments, and premiums for those eligible for National Pension Plan and Employees' Pension Insurance, defined benefits pension plans, defined contribution pension plans, mutual aid pensions, government pensions, etc.

3.2. Labor Insurance

Procedures related to notifications for those eligible for employment insurance, receipt of unemployment benefits, job-seeking at public employment offices, and workers compensation benefits

3.3. Welfare

Procedures related to applications for payment of childrearing allowance, special child allowance, special benefits for people with disabilities, etc.

Procedures related to applications and notifications for livelihood assistance

Procedures related to applications for welfare fund loans for single mother families and widows and for living welfare fund loans

3.4. Care Insurance

Procedures related to notifications, benefit payments, and premiums for those eligible for care insurance

3.5. Healthcare

Procedures related to notifications and premiums for those covered by health insurance (including short-term benefits under the National Public Officers Mutual Aid Association Act and the Local Public Officers Mutual Aid Association Act) or the National Health Insurance Act

Procedures related to applications for healthcare benefits under the Maternal and Child Health Act and the Child Welfare Act and applications for self-reliance support under the Services and Supports for Persons with Disabilities Act.

3.6. Taxes

Entry on documents directed by national tax laws to be submitted to a Tax Office Director, and related uses.

Entry on documents directed by local tax laws and related ordinances to be submitted to a local government, and related uses.

3.7. Other

Procedures related to social security and local taxes as designated by prefectural ordinances.

Ⅱ. Overview of the Circumstances of Privacy Protection in Japan

1. Overview of the Act on the Protection of Personal Information[2)]

The purpose of the Act on the Protection of Personal Information is stipulated as follows in Article 1:

The purpose of this Act is to protect the rights and interests of individuals while taking consideration of the usefulness of personal information, in view of a remarkable increase in the use of personal information due to development of the advanced information and communications society, by clarifying the responsibilities of the State and local public bodies, etc. with laying down basic philosophy,

2) See materials in English available at http://www.caa.go.jp/seikatsu/kojin/index_en.html

establishment of a basic policy by the Government and the matters to serve as a basis for other measures on the protection of personal information, and by prescribing the duties to be observed by entities handling personal information, etc., regarding the proper handling of personal information.

As noted in Article 1, the opening section of the Act on the Protection of Personal Information calls for the State and local public entities to formulate and implement measures to protect personal information, but specific provisions for administrative organs are provided in other laws. The Act on the Protection of Personal Information Held by Administrative Organs provides for the State, the Act on the Protection of Personal Information Retained by Independent Administrative Agencies and Others provides for independent administrative entities, and ordinances to protect personal information provide for local governments.

The following sections of the Act on the Protection of Personal Information lay down the general duties that must be observed by the private sector. The main duties of the private sector are stipulated to be (1) Restriction by the Purpose of Use, (2) Proper Acquisition, (3) Security Control Measures, (4) Restriction of Provision to Third Parties, (5) Disclosure, Correction, Stopping the Use. These duties were decided based on the aforementioned eight principles of the OECD. More detailed regulations exist for finance, health care, and other individual fields in the private sector through guidelines determined by the relevant ministries and agencies. These duties do not apply to small-scale entities or for personal use, or to media reports, research, religious activities, and political activities.

In order to ensure that the private sector observes these obligations, each industry draws up its own guidelines for protection of personal information, and an authorized organization for the protection of personal information handles any complaints concerning the handling of personal information made against an entity handling personal information, separately from the entity. And if the entity does not uphold its obligations, the competent minister holding jurisdiction over the entity can take measures for improvement of the situation, such as ordering that it correct or stop the violations. If the entity does not comply with the order for correction or cessation, it will be sentenced to imprisonment of not more than six months or to a fine of not more than 300,000 yen.

2. Technological Advancements and Delay in Response

Although the Act on the Protection of Personal Information has been enacted

since 2005, the issue of privacy has still not been sufficiently resolved. In society today, technological advancements have made it possible to easily grasp, store, and analyze an individual's history of behavior.

For instance, web page view history and search history on the Internet is collected and analyzed. Behavioral data is grasped by attaching cookies to the browsers of website visitors, which allows revisits to the site by the same cookie to be recognized as visits by the same individual. This is not regulated by Japan's Act on the Protection of Personal Information.

Because this Act regulates the entities those have "personal information". In this Act, "personal information" means information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).

The term in parentheses shows that the information A which cannot identify the specific individual itself fall into "personal information" when the entity who obtain the information A can easily identify the specific individual by combining it with other information. For example, a telephone number itself is not usually "personal information". Because, in Japan, it is not easy to know whose number it is from the number itself. But, if you have a database to search telephone numbers and easily know whose number it is, the telephone number could be personal information for you.

Come back to cookies, since the operator only has a history of visits by cookies, and not information that can identify the visitors, such as names, the operator is not regulated by Japan's Act on the Protection of Personal Information.

But with the accumulation of information such as browsing history, it would become easier to identify whose information this is; and even if identification is not possible now, it is likely that technological progress will make this possible in the future.

These issues raise new questions. Should we leave it unregulated when a person could be identified on the Internet without being identified in the real world? We have to make new rules for the identification on the internet. The United States is more advanced than Japan in online behavioral advertising, a form of advertising that collects and analyzes web behavior to send advertisements tailored to the tastes of an individual. In response to this, the industry is imposing self-regulations and there are also studies underway on regulatory bills. Meanwhile, in Japan, the government has just begun to argue plans for regulations.

Ⅲ. The Influence of the Number System on Privacy in Japan

1. The Privacy Problems of Identification

Amid such advancements in gathering information on an individual's history of behavior, the government is now stepping up its work to introduce the number system as I mentioned earlier.

In Japan, the Juki Net residency registry system was launched in 2003 as a national ID system, but due to concerns over privacy, it was prohibited for the private sector to ask for this number. In addition, there are hardly any cases requiring the presentation of this number to receive public services. Because of such circumstances, there is hardly anyone who knows his or her own number. Meanwhile, however, the numbers in the number system are used for tax collection purposes, it would have to be presented to the other party in the event of monetary transactions, making it clear that this will come to be used in the private sector. If this number is broadly used in the private sector, it could serve as the key to collecting personal information, and, as in the United States, lead to the development of an industry dealing in personal information.

Daniel Solove, a professor of law at the George Washington University Law School in the U.S, wrote that identification itself has privacy problems because it connects people to data, identification attaches informational baggage to people. This alters what others learn about people as they engage in various transactions and activities.

There are concerns that our society will become one in which a single piece of information can provide the means to retrieving large amounts of information about an individual.

2. Society Heading toward a Panopticon

It could be said that living in a society where new technological advancements can put your personal information on display to others, notably the government and big companies, would be like being imprisoned in a Panopticon prison building. A Panopticon prison is designed so that the prisoners in their cells are unable to tell if the observers in the observation tower are watching them or not. Imagine how it would be to have your personal information known to a person in control but you are not able to see that person. If this situation continues, you would

begin feeling that you' re being monitored at all times even when that person is not actually observing you, and this would discourage you from acting differently from other people. This kind of chilling effect leads to a loss of autonomy. It is an issue that cannot be overlooked as it shakes the foundation of democratic society, which is built on the premise of a collective body of autonomous individuals.

The German Federal Constitutional court expounded the importance of privacy as the foundation of a democratic society in its 1983 population census decision. It concluded that a person who cannot foresee with sufficient certainty how much of his or her information is known to certain segments of society, and who is not able to assess to a certain degree the knowledge of his/her communication partners, may be essentially limited in his/her liberty to plan and make decisions. A society in which the citizens can not learn who came to know what about them, and when and at what opportunity this took place, would stand against the right to informational self-determination, and this also follows for the legal order that made this possible. It goes on to say that individuals who are concerned that behavior differing from others can always be recorded, accumulated forever as information, used, and communicated, would avoid attracting attention to themselves by taking that kind of action. For example, people who know that there is the possibility of danger in participating in a meeting or civil movement, which will be recorded by the authorities, would probably not exercise their basic rights such as the freedom to meet and the freedom of expression. This sentiment not only damages the development of each individual personality, but also the public interest; the reason being that self-determination, which forms the basis for citizens to act on their own decision and supports their capability to cooperate with others, is the basic condition necessary for a free and democratic community to function.[3)]

Moreover, the Act on the Protection of Personal Information has brought Japanese society closer to a Panopticon. In a Panopticon, the flow of information between prisoners in their individual cells is obstructed. In much the same way, the Act of Protection of Personal Information has been inhibiting the flow of personal information in the private sector in a general and comprehensive manner. The provisions of Japan' s personal information act are, in principle, directed toward controlling the flow of all personal information. Based on this, all possessors of personal information—mostly government and large companies—can

3) Tsuyoshi Hiramatsu, *Kojinjyoho hogo— riron to un' yo* [Protection of Personal Information: Theory and Application] p. 26

easily refuse to provide information on the basis of protection of personal information. And those who want information—mostly the general public, media, and researchers—are not be able to obtain useful personal information even on rational grounds unless they act aggressively and devote an enormous amount of time and effort. There is an increasingly uneven distribution of personal information.

Solidarity between people is being hampered because name lists cannot be created. There have also been an increasing number of cases where the names of public officials involved in scandals are not revealed under the pretext of personal information. Speaking from my own experience, I had once requested an insurance company to provide me with a document that was prepared by a doctor upon their request concerning the injury of a client of mine, but they refused to give this to me on the grounds that it contained personal information on the doctor.

In this way, through advancement of technology and the Act on the Protection of Personal Information, a trend can be seen in Japan for certain powers to have the bulk of personal information, making it appear that Japan is heading toward becoming a Panopticon.

Ⅳ. The Path We Should Take

I now wish to propose some schemes that we should take to avoid becoming a Panopticon.

1. Redefining the Value of Privacy

I believe that the time has come for us to think once again about the value of privacy. Developments in technology change how privacy should be protected. For example, Article 35 of the Japanese Constitution, which provides for protection of all persons in their home against entries, searches and seizures, can also be considered as aiming to protect the privacy of the residence, but if there are technologies that can eavesdrop on conversations or see inside the house from outside, limits will be reached in protection under Article 35. Much of our privacy has been protected merely by existing physical elements, such as the exterior walls of a house. In a society where the advancement of technology has made the walls of a house no longer able to live up to their role of protecting privacy,

aggressive measures to protect privacy become necessary to replace the walls. In considering what form this should take, it would be necessary to pursue the meaning of privacy protection, namely, discern what kind of values privacy has been attempting to protect.

I believe that the value of privacy lies in protecting the autonomy of people. Thus it would be necessary to analyze privacy issues and, notably for those cases that make autonomous decision-making difficult, take aggressive measures to rectify the situation.

2. Privacy by Design

Many people feel that technological advancements will result in loss of privacy. It is true that technology is making astounding strides, and legislation is unable to keep pace with individual technologies. It would, however, be possible to also use this technology to protect privacy.

An example would be using the aforementioned cookies. Cookies can be used to refuse the use of cookies that track user behavior on the Internet. For surveillance cameras as well, there are technologies that can store the footage as blurred images when there is nothing out of the ordinary and restore this to sharp images when the need arises. There's also a method in which the camera begins to record images only when abnormal actions are detected such as a person suddenly running.

In this way, in the debate on protection of privacy hereon, it would be important to have technologies that are less privacy-invasive deliberately developed and adopted from the design stage. Special efforts to maintain privacy should not have to come from the side of the public; they need to be made by the developers of systems that could infringe on privacy.

This kind of thinking was broadened in scope by the concept of Privacy by Design. Privacy by Design proposes the design of technologies or systems that consider privacy. Privacy considerations include minimum use of personal information, maximum implementation of security, and strengthening the individual's power to control his or her information. In order to protect privacy within an environment undergoing significant technological advancements, it is believed necessary to also determine a comprehensive doctrine of this kind, and within each individual case, weigh the interests of the necessity of personal information against the protection of privacy, rather than having separate, specific conduct controls.

Google, Facebook, and other Internet services with large numbers of users were introduced to Japan from North America. Due to the efforts of non-governmental organizations for privacy protection and the Federal Trade Commission (FTC) of the United States, as well as the Privacy Commissioner of Canada, these services reflect to some extent the concept of Privacy by Design, and constant improvements are also being made. It is actually because of this situation that there has been little opportunity in Japan for people to take the initiative in thinking about protection of privacy on the Internet. (They tend to take protection of privacy for granted, with little interest in the methods taken to protect privacy.) However, I believe that in the near future, value will be placed on products and services excelling in privacy protection—just like environmental protection is today.

3. Establishment of a Third Party Entity for Privacy Protection

One of the reasons that can be given for why Japan is lagging behind in privacy protection is that there has been no organization to comprehensively handle Japan's privacy issues.

Studies were conducted on the establishment of a privacy commissioner when the Act on the Protection of Personal Information was enacted, but due to the silo bureaucracy of the ministries and agencies, it was decided that the respective ministers would be responsible for overseeing the protection of personal information in the private sector. A system for oversight by a minister, who is not an expert in privacy issues, is not effective.

Proactive efforts should be taken to build a social infrastructure that will minimize the risk of infringement of privacy. A third party entity should, after establishing the basic concepts for privacy protection in digital society, monitor how administrative organs are implementing concrete policies based on these concepts (e.g. privacy impact assessment). It would also have the function of giving guidance, advice, counsel, and orders concerning the situation of privacy protection, and promoting the spread of this basic concept among the private sector and the implementation of specific policies in line with this concept.

This third party entity needs to be established not just on the national level but on the local level as well. These third party entities should, in addition, play the role of bodies providing simple and fast solutions for privacy disputes with the government and private sector, and serve to promote awareness among the public on the true circumstances of personal information circulation and use, as well as the methods taken to protect privacy.

Abstract

The Influence of the Social Security and Tax Number System on Privacy in Japan

Junichiro Makita

The Japanese government is planning to introduce the Social Security and Tax Number System (“the number system”) in 2016. This will influence a lot on privacy in Japan.

The government will assign new numbers. The function of the numbers is to grasp information regarding incomes and so on and use efficiently that information for social security and taxation. Multiple institutions will share information relating to an individual by associating number system numbers and other numbers with him or her. The government will distribute IC cards to the public. The IC cards could be used for in-person identification and online authentication.

Although the Act on the Protection of Personal Information has been enacted since 2005, the issue of privacy has still not been sufficiently resolved. In society today, technological advancements have made it possible to easily grasp, store, and analyze an individual’ s history of behavior. Amid such situation, the government is now stepping up its work to introduce the number system. There are concerns that our society will become one in which a single piece of information can provide the means to retrieving large amounts of information about an individual.

It could be said that living in a society where new technological advancements can put your personal information on display to others, notably the government and big companies, would be like being imprisoned in a Panopticon prison building. If this situation continues, you would begin feeling that you’ re being monitored at all times even when that person is not actually observing you, and this would discourage you from acting differently from other people. This kind of chilling effect leads to a loss of autonomy. It is an issue that cannot be overlooked as it shakes the foundation of democratic society, which is built on the premise of a collective body of autonomous individuals.

Therefore I would like to propose some schemes that we should take to avoid

becoming a Panopticon.

First, I believe that the value of privacy lies in protecting the autonomy of people. Thus it would be necessary to analyze privacy issues and, notably for those cases that make autonomous decision-making difficult, take aggressive measures to rectify the situation.

Second, in the debate on protection of privacy, it would be important to have technologies that are less privacy-invasive deliberately developed and adopted from the design stage. Special efforts to maintain privacy should not have to come from the side of the public; they need to be made by the developers of systems that could infringe on privacy.

Third, proactive efforts should be taken to build a social infrastructure that will minimize the risk of infringement of privacy. A third party entity should, after establishing the basic concepts for privacy protection in digital society, monitor how administrative organs are implementing concrete policies based on these concepts. It would also have the function of giving guidance, advice, counsel, and orders concerning the situation of privacy protection, and promoting the spread of this basic concept among the private sector and the implementation of specific policies in line with this concept.

일본에서의 사회보장·조세번호제도가 프라이버시 보호에 미치는 영향

Junichiro Makita*

목 차

Ⅰ. 사회 보장 · 조세 번호제도 개요[1)]

일본 정부는 2016년 사회보장 및 조세번호제도(“번호제도“) 도입을 계획하고 있다. 이는 일본의 프라이버시에 많은 영향을 미치게 될 것이다. 본 저자는 우선 이 번호제도에 관해 설명하고자 한다.

1. 목적

일본 정부는 (1) 사회 보장이 정말로 필요한 사람들에게 사회 보장을 강화하고, (2) 소득세 납부와 같은 부담의 공정성을 확보하며, (3) 행정 효율성을 기하기 위해 번호제도를 채택할 것이라 설명하고 있다.

2 번호제도의 메커니즘

이 번호제도는 다음과 같은 3개의 메커니즘을 가지고 있다.

* 하라고 법률사무소 변호사, 일본)
1) 영어로도 이용 가능한 자료 참고(http://www.cas.go.jp/jp/seisaku/bangoseido/english.html)

2.1. 번호 부여

일본 정부는 4가지 유형의 기본 정보(성명, 주소, 성별, 생년월일)에 관한 최신 정보와 관련해 새로운 번호를 부여할 것이다. 이 번호의 기능은 소득 등에 관한 정보를 파악하고, 이 정보를 사회 보장 및 납세에 효율적으로 사용하기 위한 것이다.

번호제도에서의 번호에는 다음과 같은 5가지 특징이 있다.

(i) 각 개인에게는 1개의 번호를 부여한다.

(ii) 각 개인은 고유의 번호를 지니게 된다.

(iii) 번호는 민간분야 및 공공분야에 사용될 수 있다.

(예를 들어, A라는 회사가 B라는 개인에게 임금을 지급할 때 중앙정부 및 지방정부가 개인 B의 임금을 파악하기 위해 회사 A는 개인 B의 번호를 포함해 지급 내역을 정부에 보내야 한다. 따라서 개인 B는 자신의 번호를 회사 A에 제출해야 한다. 이런 의미에서 이 번호는 개인 B에서부터 회사 A(민간 분야), 그리고 중앙정부 및 지방정부(공공 분야)까지 사용되게 된다.)

(iv) 번호는 육안으로 확인될 수 있다(회사 A는 개인 B가 제출한 번호를 확인할 필요가 있다).

(v) 번호는 4가지 유형의 최신 정보와 관련이 있다.

2.2. 정보 공유

복수의 기관이 관련 번호제도의 번호를 이용해 개인과 관련된 정보 및 기타 번호를 공유하게 된다(우리는 이미 연금번호제도와 같은 다른 번호제도를 갖고 있다). .

정보 공유에 있어, 어떤 데이터베이스가 다른 기관이 지니고 있는 데이터베이스에 있는 특정 정보를 필요로 할 때, 이 기관은 어떤 형태의 식별자를 사용하여(이는 번호제도의 번호가 아니다. 식별자는 번호제도의 번호와 주기넷 ((주민기본대장네트워크시스템 번호))로 만들어진다) 해당 개인을 특정한 다음 새로운 정보를 얻는다.

기관들은 공유되는 개인 정보의 유형을 식별하고 공유 이유를 파악하기 위해 정보 공유 인프라를 사용해야 한다.

2.3. 식별

일본 정부는 일반인들에게 IC 카드를 배포할 것이다. 이 카드의 표면에는 4가지 유형의 기본 정보와 얼굴 사진이 표시된다. IC 카드는 또한 번호를 기록한 IC 칩이 있다. IC 카드는 개인의 식별과 온라인 인증 용도로 사용될 수 있다.

3. 통지와 번호 사용을 포함한 절차의 범위

다음에서는 일반인들이 이 번호를 제공, 사용하는 다양한 분야에서의 절차의 범위에 관한 내용이다.

3.1. 연금

국가 연금, 근로자 연금 보험, 확정 퇴직 연금, 확정 기여형 연금, 상조 연금 및 정부 연금 등의 대상자를 위한 통지, 퇴직 급여 및 보험금 등과 관련된 절차

3.2. 고용 보험

고용 보험 대상자 통지, 실업급여 수령, 공공 채용 사무소에서의 구직 및 근로자 보상 혜택 등과 관련된 절차

3.3. 복지

육아 수당, 특별 육아 수당, 장애자를 위한 특별 혜택 신청 등과 관련된 절차
생활 지원금 신청 및 통지와 관련된 절차
싱글맘 가족 및 미망인을 위한 복지 기금 대출과 생활 복지 기금 대출 신청과 관련된 절차

3.4. 요양보험

요양 보험 대상자의 통지, 급여 지급 및 보험금 등과 관련된 절차

3.5. 건강보험

건강 보험(국가 공무원 상조회법 및 지방 공무원 상조회법에 따른 단기 급여 포함) 또는 국가 건강보험법 적용 대상자들의 통지 및 보험금과 관련된 절차
모자건강법 및 아동 복지법에 따른 건강보험 급여 신청, 장애인을 위한 서비스 및 지원법에 따른 자조 지원 신청과 관련된 절차

3.6. 세금

세무서장에 제출할 국가 세법에 지정된 문서 기입 및 관련 용도
지방정부에 제출할 지방세법에 지정된 문서 기입 및 관련 용도

3.7. 기타

현 시행법에서 지정한 사회 보장 및 지방세와 관련된 절차

Ⅱ. 일본의 프라이버시 보호 상황 개요

1. 개인정보보호법 개요

개인정보보호법의 목적은 아래 1조에 제시되어 있다:

이 법의 목적은 정보 및 통신 사회의 발전에 따른 개인정보사용이 크게 증가하고 있는 상황에서 개인 정보의 유용성을 고려함과 동시에 국가나 정부 공공 기관 등의 책임을 명시하고 개인 정보 보호에 관한 기본 철학을 수립하고 정부의 기본 방침을 정하며 개인정보보호에 관한 기타 조치의 기초로 사용될 수 있는 문제들을 규정하고, 개인 정보를 다루는 기관이 개인 정보를 다루는데 있어 준수해야 하는 의무를 규정함으로써 개인의 권리와 이익을 보호하기 위한 것이다.

1조에 언급한 것과 같이, 개인정보보호법의 첫 조항은 국가와 지방 공공 기관이 개인 정보를 보호할 수 있는 조치를 마련해 이를 시행할 것을 요구하고 있지만, 행정 기관들을 위한 구체적 조항들은 다른 법에 제시되어 있다. 행정기관이 보유하는 개인정보의 보호에 관한 법률(Act on the Protection of Personal Information Held by Administrative Organs)은 주 정부를 대상으로 하고, 독립행정기관 등이 보유하는 개인정보의 보호에 관한 법률(Act on the Protection of Personal Information Retained by Independent Administrative Agencies and Others)은 독립적인 행정 기관에, 개인 정보 보호를 위한 조례는 지방 정부에 해당되는 구체적 조항을 제시하고 있다.

개인정보보호법의 다른 조항에서는 민간 분야가 준수해야 하는 일반 의무를 규정하고 있다. 민간 분야의 주요 의무는 (1) 사용 용도에 따른 제약, (2) 적절한 취득, (3) 보안 통제 조치, (4) 제 3자에의 제공 제약, (5) 공개, 시정 및 사용 중지 등이다. 이러한 의무들은 앞서 언급했던 OECD의 8가지 원칙에 기초해 정해진 것들이다. 해당 정부 부서와 기관이 정한 지침을 통해 금융, 건강보험 및 기타 민간 분야의 개별 분야에 관한 보다 자세한 규정들이 제시되어 있다. 이러한 의무들은 소규모 단체나 개인용도 또는 언론 보도, 연구, 종교 활동, 정치 활동 등에는 적용되지 않는다.

민간 분야가 이러한 의무를 준수할 수 있게 하기 위해, 각 산업체에서는 자체적

인 개인 정보 지침을 마련하고 있으며, 개인 정보 보호 승인 기관에서는 개인 정보를 취급하는 기관에 대해 제기된 개인 정보 취급에 관한 불만을 그 단체와는 별도로 다루고 있다. 그리고 만약 그 기관이 의무를 준수하지 않은 경우, 그 기관을 관할하는 해당 정부 부서장은 위반 사항을 시정하거나 중지하라는 명령과 같이 상황 개선을 위한 조치를 취할 수 있다. 그 기관이 시정이나 중지 명령에 따르지 않는 경우, 최대 6개월의 징역형이나 최대 30만엔의 벌금형에 처해지게 된다.

2 기술 진보 및 대응 지체

개인정보보호법이 2005년부터 시행되고 있지만, 프라이버시 문제는 아직 충분히 해결되지 않고 있다. 오늘날 우리 사회에서의 기술 진보는 개인행동기록을 쉽게 파악, 보관, 분석할 수 있게 만들었다.

예를 들어, 웹 페이지 뷰 히스토리나 인터넷에서의 히스토리 검색을 통해 개인행동 기록을 수집, 분석하고 있다. 행동 데이터는 웹 사이트 방문자의 브라우저에 쿠키를 심어 파악할 수 있으며, 이를 통해 동일한 개인이 방문한 것으로 인식되는 동일 쿠키에의 재방문이 가능해지게 되어 있다. 일본의 개인정보보호법에서는 이러한 문제에 대한 규정이 마련되어 있지 않다.

이 법은 개인 정보를 갖고 있는 기관들에 관한 규정만을 담고 있다. 이 법에서 “개인 정보“란 성명, 생년월일 또는 기타 개인 정보에 포함되어 있는 내용을 통해 특정 개인을 식별할 수 있는 살아 있는 개인에 관한 정보(다른 정보를 쉽게 찾아볼 수 있으며, 따라서 특정 개인을 쉽게 식별할 수 있는 정보 포함)를 의미한다.

괄호 안에 있는 용어는 특정 개인 자체를 식별할 수는 없는 A라는 정보도 이 A라는 정보를 획득한 자가 이 정보를 다른 정보와 조합해 특정 개인을 쉽게 식별할 수 있는 경우에는 개인 정보의 범주에 포함된다는 사실을 보여주고 있다. 예를 들어, 전화번호 그 자체는 일반적으로 “개인 정보“ 가 아니다. 일본에서는 전화번호 자체로 그 번호가 누구의 전화번호인지를 쉽게 알 수 없기 때문이다. 하지만, 만일 전화번호를 검색해서 그 번호가 누구의 번호인지를 알 수 있는 데이터베이스를 가지고 있다면, 이 경우 전화번호는 개인 정보가 될 수 있다.

다시 쿠키 문제로 되돌아가보면, 운영자는 쿠키 별로 방문 히스토리를 알 수 있기 때문에, 운영자는 일본의 개인정보보호법의 규제를 받지 않는다.

하지만 브라우징 히스토리와 같은 정보가 축적되면, 누구의 정보인지를 식별하는 것이 더 쉬워지게 되기 때문에, 기술 진보를 통해 앞으로는 개인을 식별하는 것이 가능해질 수도 있다.

이러한 문제는 새로운 질문을 제기하고 있다. 실제에서는 식별되지 않은 어떤 사람을 인터넷 상에서는 식별할 수 있을 때 이 문제를 규제하지 않아야 하는가? 하는 문제가 그것이다. 우리는 인터넷 상의 식별에 관한 새로운 규정을 만들어야 한다. 미국은 온라인의 행동 광고, 즉 웹 행동을 수집/분석해서 개인의 취향에 맞는 광고

로 내보내는 형태의 광고에 관해 일본보다는 좀 더 발전되어 있다고 할 수 있다. 이에 대한 대응으로, 산업체에서는 자체 규제를 하고 있고, 또한 규제 입법에 관한 연구도 진행 중에 있다. 한편 일본에서는 이제 막 정부 차원에서 규제 방안에 관한 논의를 시작한 상태이다.

Ⅲ. 일본의 번호제도가 프라이버시에 미치는 영향

1. 식별이라는 프라이버시 문제

개인의 행동 기록에 관한 정보를 수집하는 기술이 발전해가고 있는 가운데, 일본 정부는 이제 본 저자가 앞에서 언급했던 것과 같이 번호 제도를 도입하기 위한 작업에 착수했다.

일본에서는 주기넷 주민기본대장네트워크시스템이 국가 ID 제도로 2003년에 발족되었지만, 프라이버시에 관한 우려로 민간부문에서는 이 번호를 묻는 것을 금지하고 있다. 또한 공공 서비스를 받기 위해 이 번호를 제시해야 하는 경우도 거의 없다. 그러한 상황 때문에 자신의 번호를 알고 있는 사람이 거의 없다. 한편, 번호제도에서의 번호는 세금 징수 목적으로 사용되고 있어, 금전 거래의 경우 상대에게 이 번호를 제시해야 하기 때문에, 민간 분야에서 이 번호를 사용해야 할 것이 분명해지고 있다. 만일 이 번호를 민간 분야에서 광범위하게 사용하게 된다면, 이 번호는 개인 정보를 수집하는 키가 될 수 있으며, 미국에서와 같이 이는 개인 정보를 취급하는 산업의 탄생으로 이어지게 될 것이다.

미국 조지 워싱턴 대학 법대 교수인 다니엘 솔로브(Daniel Solove)는 식별 자체가 프라이버시 문제를 안고 있는데, 그 이유는 식별은 사람을 데이터와 연결하고, 식별은 사람들에게 정보 뱃지를 달아주는 것이기 때문이다라고 적고 있다. 이는 사람들이 다양한 거래 및 활동에 관여하면서 사람에 관해 알게 되는 내용을 변경시키게 된다.

우리 사회가 한 조각의 정보로도 어떤 개인에 관해 많은 정보를 알 수 있게 되는 사회가 될 수도 있을 것이라는 우려가 있다.

2. 사회의 “판옵티콘(Panopticon)”화

새로운 기술의 진보로 인해 자신의 개인 정보가 다른 사람에게 공개되고, 특히 정부와 대기업에 공개되어 마치 판옵티콘 감옥 건물에 수감되어 사는 것과 같이 될 수도 있다. 판옵티콘 감옥은 감시 타워에 있는 감시자가 죄수들을 감시하는지 아닌지를 죄수들이 알 수 없게 설계된 감옥이다. 자신의 개인 정보가 통제력을 지닌 사

람에게 알려지고 있지만 그 사람을 알 수 없는 상황에 있다고 가정해보라. 만일 이러한 상황이 계속된다면, 실제 그 사람이 자신을 감시하고 있지 않아도 자신이 늘 감시당하고 있는 것 같은 느낌을 받게 될 것이며, 이는 다른 사람과 다르게 행동하는 것을 억제하게 될 것이다. 이러한 종류의 위협 효과는 자율성의 상실로 이어진다. 이 문제는 자율적인 개인의 집합이라는 전제 하에 구축된 민주 사회의 근간을 흔들 수 있는 문제이기 때문에 간과할 수 없는 문제라 할 수 있다.

독일연방헌법재판소에서는 1983년 인구 조사 판결에서 민주 사회의 기초로서 프라이버시의 중요성을 설명하고 있다. 독일연방헌법재판소는 자신의 정보가 사회의 특정 분야에 얼만큼 알려져 있는지 충분히 확신할 수 없는 사람과 자신의 의사소통 상대에 관한 지식을 평가할 수 없는 사람은 본질적으로 의사결정을 계획하고 의사결정을 내리는데 있어 자유를 구속당하고 있는 사람이라 말할 수 있다고 판결하였다. 시민들이 누가 자신에 대해 알게 되고 언제, 어디서 그런 기회가 발생하는지를 알 수 없는 사회는 정보의 자기 결정권에 반하는 사회이다. 또한 다른 사람과 다른 행동이 항상 기록될 수 있고, 정보로 지속적으로 축적되어 사용되고 의사소통 될 수 있다는 것을 우려하는 사람들은 다른 사람과 다른 행동을 취함으로써 자신에게 주의가 집중되는 것을 피하려 할 수도 있다. 예를 들어, 회의나 시민운동에 참여하는 것은 위험성을 내포하고 있으며 당국이 이를 기록할 수 있다는 사실을 아는 사람들은 아마도 집회 및 표현의 자유와 같은 기본 권리를 행사하지 않을 가능성이 클 것이다. 이러한 정서는 각 개인의 개성 발현을 위협할 뿐 아니라 공공의 이익에도 해가 될 수 있다. 그 이유는 시민들이 자기 스스로의 결정에 따라 행동하고 다른 사람과 협력하는데 자신의 역량을 사용하는 것의 기초가 되는 자기 결정권이야말로 자유롭고 민주적인 공동체가 기능하기 위한 기본 조건이기 때문이다.

뿐만 아니라 개인정보보호법은 일본 사회를 판옵티콘에 좀 더 가깝게 다가가도록 만들었다. 판옵티콘에서는 죄수들 간의 정보의 흐름이 차단된다. 이와 마찬가지로 개인정보보호법은 민간 분야에서의 개인 정보의 흐름을 일반적, 포괄적인 방식으로 억제하고 있다. 일본의 개인정보법 조항은 원칙적으로 모든 개인 정보의 흐름을 통제하는 방향으로 이루어져 있다. 이에 기초해 개인 정보를 지니고 있는 모든 사람들(주로 정부 및 대기업)은 개인 정보의 보호라는 이유로 정보 제공을 쉽게 거부할 수 있다. 그리고 이 정보를 원하는 사람들(대부분 일반 대중, 언론 및 연구자들)은 공격적으로 행동하지 않거나 엄청난 시간과 노력을 기울이지 않으면 합리적인 이유에서도 유용한 개인 정보를 얻을 수가 없다. 개인 정보의 분포 불균형이 더욱 커지고 있는 것이다.

사람들 간의 연대는 명단을 만들 수 없어 어려워지게 된다. 또한 스캔들에 연루된 공무원 명단을 개인 정보 맥락에서 공개할 수 없는 경우들이 점점 더 늘어나고 있다. 본 저자의 경험을 얘기하자면, 본 저자는 보험 회사에 내 의뢰인의 부상에 관해 보험사가 요청해 의사가 작성한 문서를 내게 제공해달라고 요청을 한 적이 있다. 하지만 보험 회사는 이 문서를 내게 제공해주는 것을 거부했는데, 그 근거는 그

문서에는 의사의 개인 정보가 포함되어 있기 때문이라는 것이었다.

기술의 진보와 개인정보 보호법을 통해 이런 식으로 특정 권력이 수많은 개인 정보를 소유해 일본 사회가 판옵티콘을 향해 가는 현상이 벌어지고 있는 것을 알 수 있다.

Ⅳ. 우리가 취해야 하는 경로

이제 판옵티콘이 되는 것을 피하기 위해 취할 수 있는 몇 가지 방안을 제안하고자 한다.

1. 프라이버시 가치의 재정립

본 저자는 이제 프라이버시의 가치에 대해 다시 한 번 생각해볼 때가 되었다고 생각한다. 기술 발전은 프라이버시를 어떻게 보호해야 하는지를 바꾸어 놓았다. 예를 들어 주택 침입, 수색 및 감금으로부터 보호를 받을 권리를 규정하고 있는 일본 헌법 제 35조는 또한 주거의 프라이버시를 보호하기 위한 조항으로 간주될 수 있지만, 대화를 엿듣거나 외부에서 집안 내부를 들여다볼 수 있는 기술이 있다면, 헌법 제 35조가 보호할 수 있는 범위에도 한계가 있을 것이다. 지금까지 프라이버시의 상당 부분은 집의 외벽과 같은 물리적 요소를 통해 보호되어 왔었다. 기술 발전으로 벽과 같은 것에 더 이상 프라이버시를 보호해주는 역할을 기대할 수 없는 사회에서는 벽을 대신해 프라이버시를 보호할 수 있는 공격적인 방안이 필요하다. 우리가 취해야 하는 형태를 고려하는데 있어 프라이버시 보호의 의미, 말 그대로 어떤 종류의 프라이버시 가치를 보호하고자 하는 것인지를 분별해내는 것이 필요할 것이다.

본 저자는 프라이버시의 가치는 사람들의 자율성을 보호하는 것에 있다고 생각한다. 따라서 프라이버시 이슈를 분석하고, 특히 자율적인 의사 결정이 어렵고 상황 개선을 위해 공격적 조치를 취해야 하는 상황에서의 프라이버시 이슈를 분석할 필요가 있을 것이다.

2. 계획에 의한 프라이버시

많은 사람들이 기술 진보로 인해 프라이버시를 침해 당할 것이라 느끼고 있다. 기술은 놀라운 속도로 발전하고 있어 입법이 개별 기술을 따라잡지 못하고 있는 것이 사실이다. 하지만 그러한 기술을 이용해 프라이버시를 보호하는 것도 가능할 수 있을 것이다.

그 한 예로, 위에서 언급한 쿠키를 이용하는 방법이 있다. 쿠키를 이용해 인터넷상의 사용자 행동을 추적하는 쿠키 사용을 거부할 수도 있다. 감시 카메라의 경우도 마찬가지로, 비일상적인 것이 없는 경우 이미지를 흐리게 해서 비디오 클립을 저장했다가 필요하면 다시 선명한 이미지로 복원할 수 있는 기술도 있다. 또한 어떤 사람이 갑자기 뛰는 행동을 보이는 것과 같이 비정상적인 행동이 감지될 때에만 카메라가 기록을 시작하는 방법도 있다.

이렇듯 지금까지 프라이버시에 관한 논쟁에서는 설계 단계에서부터 의도적으로 프라이버시 침해가 적은 기술을 가지는 것이 중요하다 할 수 있다. 프라이버시를 보호하기 위한 특별한 노력은 일반 대중이 기울여야 하는 것이 아니라, 프라이버시를 침해할 수 있는 시스템 개발자가 기울여야 하는 것이다.

프라이버시라는 개념을 설계 단계에서부터 확장한다는 측면에서 이러한 유형의 사고방식이 확장되어 왔다. 계획에 의한 프라이버시라는 개념에서는 프라이버시를 고려한 기술이나 시스템의 설계를 제안한다. 프라이버시 고려사항에는 개인 정보의 사용 최소화, 보안 시행의 최대화, 개인이 자신의 정보를 통제할 수 있는 권한의 강화 등이 포함되어 있다. 기술 진보가 유의미하게 진행되고 있는 상황에서 프라이버시를 보호하기 위해서는 이러한 종류의 종합적인 원칙을 정할 필요가 있으며, 각 개인의 경우에 있어서는 별도의 특정 행동 통제 보다는 프라이버시 보호 대해 개인 정보의 필요성이 지니고 있는 유익성을 더 중시할 필요도 있다.

사용자 수가 많은 구글, 페이스북 및 기타 인터넷 서비스들이 북미에서 일본으로 도입되었다. 비정부 단체와 미국의 연방거래위원회의 프라이버시 보호 노력 및 캐나다의 프라이버시 위원회의 노력에 의해 이러한 인터넷 서비스들은 어느 정도 설계 단계에서부터 프라이버시를 고려한다는 개념을 반영하고 있고, 또한 지속적인 개선 노력도 기울이고 있다. 일본인들이 주도적으로 인터넷상의 프라이버시 보호에 관해 생각해볼 기회가 적었던 것도 사실은 그러한 상황 때문이기도 했다(일본인들은 프라이버시 보호를 당연하게 생각하는 경향이 있지만 프라이버시 보호를 위해 취해야 할 방법에 대해서는 관심이 적다). 하지만 본 저자는 가까운 미래에는 프라이버시 보호에 우수함을 보이는 제품과 서비스에 더 큰 가치를 두게 될 것이라 믿고 있다(현재 환경 보호에 가치를 두고 있는 것과 같이

3. 프라이버시 보호를 위한 제 3자의 수립

일본인들이 프라이버시 보호 문제에서 뒤쳐진 이유 중의 하나는 종합적으로 일본의 프라이버시 문제를 다루는 기관이 없었기 때문이라 할 수 있다.

개인정보보호법을 제정할 때 프라이버시 보호위원회 설립에 관한 연구를 실시했지만, 정부 부처의 관료주의로 인해 민간 분야에서의 개인 정보보호 감독을 해당 부처가 책임지는 것으로 결정되었다. 프라이버시 문제에 전문성이 없는 정부부처별 감독 체계는 효과적이지 않다

프라이버시 침해를 최소화할 수 있는 사회적 인프라를 만들기 위해서는 선제적 노력을 기울여야 한다. 디지털 사회에서의 프라이버시 보호에 관한 기본 개념을 수립한 뒤 제 3자가 행정 기관이 그러한 개념에 기초해 구체적 방침을 어떻게 시행하고 있는지를 감시해야 한다(예: 프라이버시 영향 평가). 또한 제 3자는 프라이버시 보호 상황에 관한 지침, 자문, 조언, 명령 등을 제공해야 하며, 민간 분야에 그러한 기본 개념을 홍보하고, 그러한 개념에 부합해 구체적 지침을 시행해나갈 수 있게 해야 한다.

제 3의 기관은 국가 차원에서뿐 아니라 지방 차원에서도 수립되어야 할 필요가 있다. 이 제 3의 기관은 또한 정보와 민간 분야에 프라이버시 관련 분쟁에 대해 간단하면서도 빠른 솔루션을 제공해주는 역할과 일반 대중들이 개인 정보 배포 상황과 그 사용 및 프라이버시 보호를 위해 취해야 할 방법에 관한 인식을 촉구하는 역할도 담당해야 할 것이다.

국문초록

일본에서의 사회보장・조세번호제도가 프라이버시 보호에 미치는 영향

Junichiro Makita

일본 정부는 2016년 사회보장 · 조세 번호제도 ('번호 제도') 도입을 계획하고 있다. 이는 일본의 프라이버시 문제에 많은 영향을 미치게 될 것이다.

일본 정부는 새로운 번호를 부여하게 될 것이다. 이 번호의 기능은 수입 등에 관한 정보를 파악해 이 번호를 사회 보장 및 세무에 효율적으로 이용하기 위한 것이다. 복수의 기관들이 관련 번호 시스템 번호를 통해 각 개인에 관한 정보를 공유하게 될 것이며, 그 개인에 관한 다른 번호들도 공유하게 될 것이다. 정부는 일반인들에게 IC 카드를 배포할 것이다. 이 IC 카드는 개인의 식별 및 온라인 인증 용도로 사용될 것이다.

비록 개인정보보호법이 2005년 이후부터 시행되고 있지만, 프라이버시 문제는 아직 충분히 해결되지 못하고 있다. 오늘날의 사회에서 기술 진보는 개인의 행동 기록을 쉽게 파악, 저장 분석하는 일을 가능하게 하였다. 이런 상황에서 일본 정부는 이제 번호제도를 도입하기 위한 작업에 착수하였다. 우리 사회가 하나의 단일 정보로도 개인에 관한 많은 양의 정보를 인출할 수 있는 사회가 될 것이라는 우려도 있다.

새로운 기술 진보를 통해 우리 자신의 개인 정보가 다른 사람에게 공개되고, 특히 정부 및 대기업에 공개되는 사회는 판옵티콘(Panopticon) 감옥 건물과도 같은 사회가 될 수 있을 지도 모른다. 이러한 상황이 계속된다면, 우리는 실제로 관찰 당하지 않아도 늘 감시를 받는 것과 같이 느낄 수 있을 것이며, 이는 다른 사람과 다르게 행동하는 것을 억제할 수도 있다. 이러한 위협 효과는 자율성의 상실로 이어지게 된다. 이 문제는 자율성을 지닌 개인들의 집단으로 이루어진 민주사회의 근간을 흔들 수 있는 문제이기 때문에 간과할 수 없는 문제라 할 수 있다

따라서 본 저자는 판옵티콘이 되는 일을 피하기 위해 우리가 취해야 하는 몇 가지 제도를 제안하고자 한다.

첫째, 본 저자는 프라이버시의 가치는 사람들의 자율성을 보호하는 것에 있다고 믿는다. 따라서 프라이버시 이슈, 특히 자율적인 의사결정을 어렵게 하고, 상황을 시정하기 위해 공격적 조치들이 필요한 사례에 있어서의 프라이버시 문제를 분석해

볼 필요가 있을 것이다.

둘째, 프라이버시 보호에 관한 논쟁에서 설계 단계부터 프라이버시 침해가 적은 기술을 의도적으로 개발하고 채택하는 것이 중요할 것이다. 프라이버시를 보호하기 위한 특별한 노력을 대중들이 기울일 필요가 없어야 한다. 그러한 노력은 프라이버시를 침해할 수도 있는 시스템 개발자가 기울여야 하는 노력들이다.

셋째, 선제적 조치를 취해 프라이버시 침해 위험성을 최소화할 수 있는 사회 기반구조를 갖추어야 한다. 제 3자는 디지털 사회에서의 프라이버시 보호라는 기본적 개념을 수립한 이후 행정 기관들이 그러한 개념에 기초해 구체적 방침들을 실행하는 과정을 감시해야 한다. 또한 프라이버시 보호 상황에 관한 지침, 자문, 충고, 명령 등을 제시할 수 있는 기능을 갖추고, 민간 분야에서 그러한 기본 개념을 홍보하고 그러한 개념에 부합되게 구체적 정책을 시행할 수 있게 해야 할 것이다.

제3주제

최근 국제 디지털 생태계에서 자유를 보장하기 위해 어떤 긴급한 조치를 취할 것인가

Which Urgent Initiatives to be Taken to Safeguard Our Freedoms with Regard to the Current Worldwide Digital Developing Ecosystem

Marie Georges[1)]

Overview

Preliminary Thankful Words

I would like to express my gratitude and how honoured I fill by invited by the Institute of legal Studies of Konkuk University to share in South Korea my experience and thoughts. It is also emotional as it is the fourth time I am invited in Korea since 2002[2)]. on different topics related to "ITC and freedom" legal

1) independent expert in "ICT and Human Rights", France, Europe
Member of the "FREE Group" (The Fundamental Rights European Expert Group associates academics and experts of several EU countries focusing on monitoring, teaching and advocating in the European Union freedom, security and justice related policies); scientific expert for the Council of Europe in modernizing the DP convention and for promoting DP; former adviser for development and foresight of the chairman of the French independent "ICT and Freedom" Commission (Data Protection Authority), former member of the European Commission's unit in charge of elaborating the DP directive of 1995.Economist working for the learning centre at the national research centre for computer sciences (INRIA), she was in the small activists team in 1973-78 for the adoption in France of the 1978 DP law, then recruited by CNIL for helping organizing the staff and for the application of the law in different sectors.

system of protection, as being French I use and like to say. On international level the words of "Data Protection" or "Data privacy" are more common and historical, but not well tailored in my view with regard to what is at stake as we see it now quite well.

INTRODUCTION – The challenges, Origin, Urgent Initiatives for Effective Solutions

1. Information and communication technologies (ICT) are moving fast from a number of perspectives: local, regional, international in the fields of ICT research, working division and use together with different methods of design (open source/proprietary), different economic models, huge competition.

Along with the extension of use of ICT and ICT innovations[3] within our daily life, for work, hobbies, relations, frequent or exceptional activities personal or collective or personal, more and more of all our different but freedoms and fundamental rights are at stake while being interconnected, privacy, right to association, right to information, to religion belief, to move freely (location data) …while even dignity and the right to resistance are now be at stake. As a result the so called "Data Privacy Protection" is more and more the basic right and mean to safeguard the exercise of all our human rights in the digital space connected to real life.

From my 40 years of experience in DP as practitioner, the concrete desired solutions to save guard our interconnected Human Rights with regard to ICT are very close everywhere with no much "cultural distances" but the possibly to implement them in concrete legal system relates to precise legal system and vision at a certain time together with political rapport de force locally and internationally.

As a matter of facts, it can be demonstrated that the general basic principles

2) I was invited first in Korea for a conference in 2002 held by the KISA while the first Korean Data privacy law was in the course of elaboration; then in 2009 by the KHRC before second DP law was adopted in Korea, which established a second DP regulatory authority; then in November 2012 for three DP events, invited by the Sung Kyun Kwan University, the Korean Constitutional Law Association, the Personal Information Protection Law Association and by the Personal Information Protection Commission.

3) According to experts, all the today operated IT did not exist 10 years ago and 50% of the nanotechnologies will be in the field of IT.

called either “Fair information practices”, “data protection”, “data privacy “or” ICT and freedoms”, first established in the 70s[4], are still fully meaningful, but because of there implementation in particular legal system at a particular time, the first urgency is to assess up to which point our precise legal enforced DP systems to implement them at a certain time, mostly dated in the 90’s and 2000’s, are still efficient or not, including at technical level, and as a consequence to identify which gaps arise and how to fulfil them.

In a word, in order to get a sustainable data privacy in a changing world mostly due to evolving IT and services within national boundaries, regionalisation and globalisation, it is necessary to assess regularly the legal framework in which we operated to make it evolving for effective protection of our human rights.

2. I intend to share with you today the identification of the gaps and possible solutions by confronting the different components of all our ‘ICT and freedoms’ laws (definitions/scope, basic safeguards /obligations of those designing, producing, or handling personal data, complementary safeguards /individual’s rights, principles related to transfer of personal data to foreign countries, institutional independent mean for enforcement, international cooperation) to concrete examples taken in those marketing designated areas of personal data processing “blogs”, “forum”, “social networks”, “search engine”, “cloud computing”, “big data”, “internet of things”, to new types of very intrusive data being now processed and new types of processing (such as digital fingerprints, DNA, facial recognition), also in areas of e governmental policies (e health, electronic passport, digital fingerprints, DNA …). The explosion of personal data processing leads mainly to assess the mechanisms of the governance and to complement them.

3. Because more and more personal data processing are international and spread between different actors differently located, to be short, from the user device or equipment (smartphone/app, laptop/software, computer/software), to the network

4) See on Bog Gellman ‘s web site the US history of the FIP, lastly updated in June 2013, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.
In EU and on international level the First Data Protection Law was adopted lin 1970 in Land Hessen – Germany, the first national DP Law in 1973 in Sweeden, the French « Informatics and Freedoms » Law was adopted in 1978. On international level the OCDE DP Guidelines were adopted in 1980, Council of Europe’s convention 108 was adopted in 1981, UN Guidelines for national DP Law (in line with the CoE’s convention) were adopted unanimously by the General Assembly in 1990, the EU directive on Data protection which developps Convention 108 was adopted in 1995

(…), the platform offered by cloud computing entities to the recipients though their equipments for the particular purpose of the personal data processing at stake, it becomes obvious that:

3.1. The design and implementation of each of the elements in the chain of the data processing at stake, has to contribute to the overall data processing by taking care of the data protection principles. So all the different kind of actors involved in the processing operations of personal data must be under coherent obligations.

3.2. To obtain such result, from a national point of view more and more extraterritorial legal needs occur which are filled today by the famous EU " adequacy level of protection principle" through assessment of the recipient country legal framework, or its pragmatic solutions through contacts and binding corporate rules together with exceptional safeguard in case of need, so the users/data subject rights go along her/his data.

4. With the acceleration in the number of States in the world having adopted DP laws, up to reach 101 last month, according to our friend Graham Greenleaf [5], conflicts of DP laws, or conflict with new regional DP laws may occur.

To solve those conflicts in such a multi dimensional context, the need and the urgency to cooperate within an international binding data protection instrument including governance mechanisms and means to make it evolving is raised. In parallel a two regions initiative is exploring pragmatic arrangements (EU/APEC data protection authorities), and a "interoperable legal systems" concept is promoted (USA). This latter miracle communication mixture of technical and legal concepts may leave politically doubtful some of us.

For the moment, as long as the UN does not move in that direction since the adoption unanimously by the General Assembly in 1990 of non binding "Data Protection Guide lines" [6], and if it could shortly move according to some recent political initiatives from NGO and Governments it would take another 10 or 15

5) 8 countries has DP law in the 1970s, +13 in the 1980s, +21 in the 1990s, +35 in the 2000s, +24 in only2000-2013, so by September 2013 101 countries have DP laws comprehensive covering all sectors, some only private sectors and some only public sectors. Graham Greenleaf, Sheherezade and the 101 Data privacy Laws, Origins, Significances and Global trajectories, September 2013 http://papers.ssrn.com/sol3/papers.cfm?abstractid=2280877

6) Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990

years to reach an agreement, only its precursor the Convention 108 of the Council of Europe of 1981, open to third countries and which is in a final step of modernization too[7], currently plays that role. This adhesion by non European countries should interest Asian countries as it does currently African (already Morocco) and Latin American countries (already Uruguay) and more and more countries out of Europe are asking to be observer it in order to cooperate with all the Parties on its application, in a common way, to particular new kind of emerging data processing. This modernized convention will also for the first time in the world allow all Parties' data protection authorities to legally exchange for enforcement matters concrete personal data where necessary in international complains related to personal data being processed in the territory of several parties for the fist time.

5. The further in deep assessment in this speech of our needed solutions will be based mostly on the current European experience where data protection has already a constitutional status, and law provisions regarding foreign world services such as Google or Facebook. The European directive on Data Protection of 1995 is since February 2012 under review for update. This exercise on the European Commission proposal for a revised DP regulation and another text for police matters should be end beginning of 2014includes over 4000 amendments in the European Parliament, mostly dictated by economic and US lobbying as expressed in media and condemned by US and EU NGO (see their Washington statement on June 24, 2013). This strategy of two texts is not at all liked by all DP European experts being in favour of only one general law which can be complemented by particular provisions where needed for particular balance of interests aspects for specific sector personal data processing (as it has been done for electronic communications for telecom directories, identification of the caller and so on). However the current European strategy is due to the particular characteristic of the European Union which is not a federation of States but a Union of States which do not share at the level of the Union all the national powers in particular in the field of national security and public order.

I will not go in those details on this EU approach along with two general texts on DP, except in the last part of my speech, on the common questions they raise

7) Proposed modernization by the committee of the convention, 18 December 2012, T-PD 201204_rev 4 http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_E_Convention%20108%20modernised%20version.pdf

and not fully satisfied on the possible limitations or derogations to the DP principles "in a democratic society" for disclosure of personal data held by private entities "as far as necessary and proportional in a democracy" to police services in the course of preventing or investigating criminal cases together processed with their own collected data, and for national security operated partly by secret services.

The Edward Snowden's revelations, after those on Echelon in 2000/2001 and alerts by US NGOs since 2005 and 2008 on NSA and PRISM, with no concrete positive result at that time on the level of establishing legal democratic principles and control, place us this time in the political and legal urgency to do so, in order to widely prevent such tragic huge loss of freedom, not to say facing such a huge treason in the name finally of pure domination over the management of infrastructure (see ICANN and the growing place taken by US world services using fiscal paradises), for cultural and economic domination.

6. As a consequence, besides the revision of our model of DP law and the world DP rules to be to be established other initiatives against that domination are needed of other nature to be taken in parallel, that are not developed in this speech, without which we will not be able to safeguard our freedom and sovereignty in the digital space, and at least:

- On the political side we have to reach agreement on world level to sanction spying other states activities through whatever mean for economic, industrial and political benefice, as it is forbidden from citizens in our democracies.
- On the technical governance we have to promote a true multilateral and multistakeholder world governance under the umbrella of UN for an open Internet, instead by an ICANN still connected to US government.
- On the industrial level we have to promote means to prevent those spying and domination through
  - National or regional "cloud computing services", and
  - Confidentiality/cryptographic techniques "end to en".

I. Assessment of the Components of DP Legal Material Principles Based on the 90's and 200's Vision, with Regard to the Evolution of IT and of Their Uses.

1. The Link between ICT and the Basic Principles of Data Protection

What is the aim of "Data protection" : it is to PREVENT abuse of use of personal data in the hand of others (employers, commercial entities, banks, public authorities, charities, political parties, libraries and so on), having in mind that personal data being of the concerned individual personality or identity cannot be subject to "appropriation" and that the protection a stake is directly related to the protection of human being.

Those possible abuses originate in the easy way and at low cost digitalised personal data may be collected even without the individual concerned knowledge (i.e. video-surveillance) stored for a long time (while legal prescriptions exist in the "off line world based on the right to forget), reused (i.e. for a purpose in the interest or not of the person), manipulated/changed, matched with other digitalized sources (for elaborating profiles on the basis of a common identifier, a unique identifier or even on a set of same data in the different files, to take decision on the basis of such profile with regard to the individuals concerned in the commercial field, in the police or justice field?), transmit even far away to the other face of the earth for being process at a lesser cost, all without her/his control, or even published purposely or not, erased, loss by miss-manipulation.

So the DP principles, which had been elaborated, aim at preventing those abuses by mainly shaping the design of the processing of personal data at both the time of design of the processing operations and at their implementation.

- To those ends it is needed to define what is personal data, to fixe the list of principles is to be taken into account as rules and how in liable for applying them:

2. Main Gaps Relating to Definitions or to Their Interpretation and Possible Solutions

Personal data, was defined as "related to an individual which is identifiable" (Convention 108), "directly or indirectly by reference in particular to identification number, or to more factors specific to the physical, mental, economic, cultural, social identity " by anyone who would get to know it (EU Directive of 95 definition of the "data subject") interpreted with huge difficulties facing lobbyists' views as "who would get to know it lawfully or not".

- So "raw" data related to an individual without her/his name may lead to identify that individual depending on their content. It is well known by statisticians that the job, gender, age and home location of a person may well lead to know who is that individual by all her/his surrenders. This was being important when talking yesterday about data being anonymized for use by third person for research without under particular condition.
- This is no longer valid along with the explosion of data processed goes, as scientists showed it. The more you held personal data on one person even without the name and some of those "sociological data", the more if published, the individual will be identified. As consequences:

- It is all the more important to avoid to define what is "anonymous data" as some would like to do it currently at the EU Parliament.
- We have to find ways to apply all the DP principles to raw individual data from the bottom, the time of collection of data while some would like we forget the collection step of data from individual on order to concentrate only on the use of data. This may be important within the approach of "big data" said "anonymous" and not submitted to rules especially for statistical purposes which may be issued from them. At least in that context, massive world used services should in that perspective not permitted to elaborate hidden statistics published or not without being under a democratic control of a public interest pursue (no initiative currently on that item).

Within the telecom environment of course the definition of personal data covers the fixe line number and mobile number and all what is called as "traffic data" or "meta data" which on a long period gives such a deeply intimate vision of the individual concerned.

Moreover, the online environment leads also to the fact that without the need to know anything related to an individual expect her/his attributed IP address in real time, interaction to influence that person is possible. It is what the EU working party of DPAs, followed by the MP reporter on the DP package at the EU Parliament, names as date enabling to "single out" an individual. This precision, which as no jurisprudence basis, will certainly be added in the EU personal data definition.

Profiling: the more and more use of such techniques leads above the related safeguard already in the EU directive of 95, to more precise its definition. In that exercise the EU is taking the definition elaborated by the Convention 108 committee of the Council of Europe in a recent recommendation on the mater, as meaning "any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyze or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior".

Producer: in order to apply the DP principle to all the actors implied into the chain of designing and operating processing operations on personal data, along with its need described in our introduction, in addition to the definitions of "controller" of the personal data processing (who decide its creation) and of the "processor which is the eventual third party acting on behalf of the controller, the definition of the "producer" is proposed by the MP reporter at the EU Parliament as follows: 'producer' means a natural or legal person, public authority, agency or any other body which creates automated data processing or filing systems designed for the processing of personal data by data controllers and data processors". I hope this definition will be when adopted completed by "and by users".

3. DP Material Interconnected Principles, Which List is Well Known, Should be Applied Effectively with More and More Strength

- The fair and lawful collecting and processing principle, which means in particular no unfair way to collect data is permitted. See how normally video camera must be well signalled to individuals where lawfully operated (…) and the extended foreseen information that have to be promptly given to data subject

- The specified, explicit and legitimate purposes principle including with regard to the potential reuse of the data and to the recipients who may use the data.

  In the field of legitimacy or legal basis of the purpose/object of the processing, while up to now the basic safeguard for a data processing, the "consent of the individual concerned" was more of a theoretical nature with regard to the most numerical concrete situations in which all the other legal basis were pertinent, such as being "necessary for performing the contract" or "necessary to full a legal obligation" or "to perform its vested task by a public authority", more and more frequently the consent of the individual will have to be pertinent, in particular in relation of enterprises offering more and more online services which would like to use the data collected in the course of one service for its other services of a completely different purpose nature.

  In order to avoid in such situation of non-compatible purposes from the original purpose for collecting data, the EU Commission following most experts and NGO view, is of the opinion, which in my view will be adopted by the Parliament, that a more precise definition of the consent is now needed. The consent has to be not only specific, informed and free, as defined up to now, but also "explicit" through a data subject's affirmative action.

- The adequate, relevant and proportional principle, also called the "minimisation principle" which applies both to the nature/quantity of data being used and in their time of retention by reference to the legitimate purposes at stake.

  This principal is to play of course a more and more important role as regard for instance the retention period of data such as of location with regard to the right to move, or the request on a search engine with the right to information and own thoughts. This retention period should be by default around zero, while a longer period should be based on the free and explicit consent of the user, or by law as far as necessary for the prevention of an imminent crime or for an investigation on a serious crime (see in that later case the 3 months established by the cybercrime convention of Budapest). For those later cases, the 6 to 24 months period of retention of all user's traffic data, left to the decision of Member States, established by a specific EU directive has being challenged in several

Constitutional Courts in EU is revised. Unfortunately we are still waiting for that revision.

- The reinforced protection when "sensitive data" are at stake

  The list of data that are prohibited to be processed without consent (except where the law prohibit its use even with the consent for protecting the data subject such), or on the basic of laws providing particular safeguards is foreseen to been extended to genetic data in EU and within the modernized Council of Europe convention also to biometrics which are unique to an individual. The original list was only devoted to data which use could present the risk of discrimination: data revealing racial or ethnic origin, political opinions, the religion, the membership of a trade union, the data concerning health, the sexual life, or penal sanctions, or security measures qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale).

  Much should be known about Europe on this topic : examples

  - Regarding biometrics and genetic data: the French Constitutional Council for being disproportionate in 2012 has rejected the retention of the 10 digital fingerprints, instead of two in the related file, for obtaining the EU passport with two protected digitalized fingerprints in its RFID or an national identity card of the same nature; the argument of the 70MPs who appealed to the Constitutional Council on the related law was also on the risk of such a file on nearly all nationals with regard to the right to resistance in case of failure in the democratic state or of invasion. The Parliament of Germany decided in 2005 even, than once the EU passport was produced and issued to a German, no digital fingerprint could be retained in the file. The European Court for Human Rights in Strasbourg decided in a case against United Kingdom in 2008 that storing the genetic data and digital fingerprints in a police file related to individuals who have been found not guilty by court was in particular contrary to the innocence presumption.
  - Regarding health data: in France the disclosure of health data to a third party by a health information web site has been prohibited by law even with the consent of the individual concerned

- The security principle, applying to the personal data processed and to the software for it use, including in case of electronic transmission which is all

the more required is complemented by an obligation of fast notification to the concerned DPA in case of a security breach and to the individuals concerned as it came necessary after several important cases in several EU countries as too in United States.

- The complementary safeguards for individuals, in the form of rights they have to enjoy in order to know and control what for her/his data will be used and how.

  This is classically achieved though the different following rights:

  o Appropriate information given to the data subject at time of collection of data by the data controller

  This information is foreseen to be extended, above the name and address of the controller, the purpose of the collection of data and the recipients currently provided, to the retention period, the possible transfer of data outside of EU, and to the user friendly mean to exercise the rights, and provided promptly (not hidden behind a URL)

  o The right to access to owns data processed/stored and the right to correct or suppress in case of incomplete, erroneous, or unlawful data.

  Two major precisions are foreseen to be added:

  "The right to portability" being to obtain on line owns data in a standardized form (useful for own personal data processing or to move from one service provider to another one), and

  "The right to be forgotten", as a precision with regard to the right of suppression (to be useful in the field of published data and of de-search ability from search engines).This "new" right is much debated on the basis of freedom to speech which has of course to be taken into account, while many practical cases shows its workability and need.

  o Regarding the particular risk of automatic decision while using profiling techniques the particular safeguarded which appeared necessary in France since 1978 and provided in the EU directive of 95 , as to the right to challenge the reasoning and to add information before final decision is of course maintained(further more, such decision based on processing is absolutely forbidden in the field of judicial decision)

  o Regarding the economic advantage of reusing data for marketing purposes some balance of interests had been already done in the EU e privacy directive, according to the level of the intrusiveness of the technique used: obligation to be inform on the purpose and right to

refuse such purpose (“right to object” which is different from the US “opt out” which does not include the obligation of informing the individual concerned), when by mean of telephone or electronic communication the explicit consent of the individual is required

o One can note that in some EU Member States regarding criminal record (out of the scope of the EU), which are never publically available, the right of the individual concerned to access to her/his complete record has been limited to only consult it in order to protect individuals against pressure from others not being authorised by law to get those information.

o The right to complain to the Data Protection Supervising Authority or at the individual choice to the court.

While this right was only provided on an individual basis, it has been assessed that it should be reinforced by the possibility, foreseen to be established within the revised EU regulation, that it could be exercise, at the choice of the individual, on a collective basis through Human rights NGO and class action procedure.

II – Assessment of the Provisions Related to the Limitation to the Material Principles “as Far as Necessary in a Democratic Society”

This speech does not allow to give all details related to all the list of goals for such limitations in important public interest or for preserving rights of others.

I will comment only, because of the actuality on such limitation in the interest of national security.

Such domain is a matter of jurisprudence in Europe of the European Court of Human rights (Strasbourg) that individuals can appeal to after having passed through all the national judicial possibility. From its jurisprudence the law provided for such limitations must be clear and precise.

That law must provide:

- The list of matters which justify such derogation
- A procedure of authorisation (except in urgency) by an independent body

- In case of secret surveillance the time limit of such surveillance, extend under a new authorization.
- The a posterior control by that independent body (which members should be designated by Parliament in my view more than by the government)
- The transparency means for the public of the whole activity: annual number of cases under each goal, requested by each services in charge of, having been authorized and non authorized for which general reasons, the results of the controls operated.

And those surveillances should be operated in a completely disconnected way from judicial procedures.

This kind of precisions could be in my view added to the modernised text of Convention 108 as to in the EU data protection text, while the EU is supposed to adhere as such to the that convention, and to the European Convention on Human Rights of the Council of Europe which set up the European Court of Human rights (48 countries while EU is of 28 member states all members of the Council of Europe.

On international level

III - Assessment and Foreseen Update on the Rules Applying to Transfers of Data to Foreign Countries (or Third Countries from EU, or Non Parties to Convention 108)

- The "adequacy level of DP in a foreign country as a principle for authorizing personal to flow over requires a European decision of recognition regarding that country.

This solution is fair with regard to the individuals concerned because insuring that her/his rights will flow along her/his data.

- However all nations in the world are regrettably still not insuring such protection, while it is much progressing currently, and as you know pragmatic tools have been developed by EU based upon a previous national experience, notably the French experience.

These pragmatic solutions are of two kinds:

- Contractual solutions used by all countries in Europe in the relations between data controllers or between, and between controllers and their processors. Model of contracts has been established at the EU level.
- The other solution is based on unilateral declaration by a corporate for itself and its affiliates. We call this instrument "binding corporate rules". Their model of content and procedure to be approved by the concerned DPAs has been elaborated by the EU working party of DPAs.

  However several member states could not recognize legal status to such unilateral declaration. As this tool proved its usefulness (but the procedure proved also to be long) The European commission is proposing to give to Biding Corporate rules legal status within the revised DP text along with a simplified procedure for adoption.

This approach contains also derogations to the principle of "adequate" protection on several basis such as

- the consent of the individual concerned or
- in case the transfer is necessary in order to protect the vital interests of the individual where he/she is physically or legally incapable of giving consent.

  From my point of view the derogation by consent should only take place for a transfer in a particular case an not on the basis of repetitive transfer and it should provided that the individual is informed of the non DP protection insured.

  It is also proposed a derogation from the principle on the basic of

It is also proposed derogations on the basis of

- an important grounds of public interest; or
- for the establishment, exercise or defense of legal claims

It has been further discovered that in some procedures preparing a trial it was required to an affiliate in Europe to produce full exchange of emails or of files in USA. Plus the risk that on the extraterritorial provision of the Patriot Act data with no relation with US , about affiliates personnel where asked by some US authorities. European legal advisers to such affiliate in several cases, called its national DPA to know if it was allowed. The DPA asked to be concretely informed of the case and referred to use the procedure established in the treaty for mutual

assistance. That is why in the version of November 2011 the proposed regulation contained in such case the obligation for the controller or processor to inform the DPA, which will authorize the disclosure and informed the competent authority while the controller or processor would inform the individuals concerned of that authorization of transfer.

Surprisingly that proposal disappeared from the proposal of the European commission when published two months later.

Due to the breach of international law constituted by Prism revealed last June by Edward Snowden and published in the Guardian and the New York Times, the use of the Patriot act for getting data from US company operating in Europe, that disappeared provision which the reporter proposed even before this event by amendment, will certainly reappear soon in the adopted text by the European Parliament.

Currently, due to the Prism scandal the conference of the DPAs of Germany decided not to authorize transfers of personal data to United States.

The European Parliament is also exploring suspending

- the EC decision of adequacy for commercial sector in US called the "Safe Harbor",
- the PNR agreement in the field of aircraft reservation along which air lines are requested to send to US authorities 72 hours before departure all events on reservations to US (which includes data that the DPAs expressed as being excessive in the content and in the length of time US wanted to store them),
- and the Swift agreement on access under particular conditions to financial data on transfers to US carried out by Swift, a company based in Belgium with an affiliate in particular in US. This agreement was concluded after the Washington Post revealed the scandal in 2004 of US government accessing to data not concerning US but in the back up of the system based within the Swift affiliate in US. AT the same time it was decided with Swift to transfer its back up in Europe.

The report on investigation and recommendations by the Committee Liberties, Security and Justice of the European Parliament will be ready end of December to

be discussed in the plenary of the Parliament beginning of 2014.

IV. The Means for Effective Application of The Material Principles

The assessment in EU of those means, mainly dedicated only up to now to

- the Data Protection Supervising Authority powers (independent, prior and posterior investigation powers),
- sanctions (fines, penal sanctions) and
- remedies,

is leading to much foreseen evolutions at each level of the data controller, the processor, and the Data Protection Supervising Authority, mostly dictated by the pressure of the explosion of the number of data processing and complains, and on the EU level mostly dedicated by a strange need for more common practices and regulation :

- In order to respect principles Producers, Controllers, processors in public and private sector, are foreseen to designate Privacy officers with guarantied independence status for:
  - o Education of staff
  - o Elaborating Explicit assessment of personal data processing presenting particular risks for privacy which list is established within a European consistency mechanism on the basis of DPA's proposals
  - o Accompanying privacy by design and privacy by default design and implementation of personal data processing
  - o Establishing internal register of all data processing with the updating
  - o Alerting the head or to the DPA when necessary
  - o Answering to demand for exercising rights and complains

- the DPA, aside its "traditional tasks" of
  - o Awareness,
  - o Advice and recommendation,
  - o Review of professional codes,
  - o Investigation on the basis of complains or on its own decision (which suppose protecting those with confidentiality duties which give information to the DPA and to establish a duty of secrecy for the DPA

members and staff),

- o Monitoring new IT or practices,
- o Opinion on draft laws and regulation,
- o insuring transparency of its activity and
- o where necessary contributing to public debate, recommendation to Head of State and institutions,

is foreseen in addition

- o To no longer register and assess all notifications of personal data processing from public or private bodies.
- o But to review controller' s assessment of data processing presenting particular risks for privacy instead of complete a priori control in those domains.
- o To issue certifications (procedure to be established further on)
- o To impose fines up to 2% of the annual revenue of an enterprise. This level of fines is considerate, while much higher than in EU countries which DPA already had such sanction power, as not enough when considering current huge violations from in particular by world services which resources are mainly made of personal data. 5 % would be more adequate.

  Example: Google street view . Google was collecting secretly communication data while filming streets to be published on its service. Some DPA have already a sanction power, with limits on the level of the maximum fines as usual. The sanction they were able to impose as been the following, in 2011 in France 100 000 € in 2012 in Germany 145 000€. In the US 7 Millions of $ penalties have been imposed to Google for the same violation last in 2013.
- o In relation with cross border data flows within EU multinationals, arrangement have still to be decided on whether the DPA of the location of the headquarters will be on charge of the supervision (vision of the European Commission) while cooperation with other concerned DPAs may be in practice required according to many factors such as the location of the real decision on data processing which may be at the level of affiliates, location of needed control on the spot, legal basis shaping a particular data processing which may be of national nature and different among Member States, the interest of the individuals concerned (vision of the working party of the EU DPAs and several

experts).

Above that discussion, few experts highlight the need for cross boundaries data processing being in violation of the rules, to decide on sanction at the EU level by a special section of the European Data protection Board composed of the national DPAs and the European DP Supervisor (EDPS) competent for supervising data processing of EU Institutions

- The European Data Protection Board (ex "EU DPAs working party) will have a stronger role on the regulation level by being in charge of the consistency mechanism (in particular decision on national DPA proposal for the list of data processing presenting particular HR risks, sector recommendations, opinion on draft European commission proposal…). Its secretariat will not any longer a European Commission's structure but within the office of the European DP Supervisor.
- First list of data processing presenting particular risks which should be under the procedure of DP assessment and when in the public sector on a precise draft regulation or law:
  - Data processing to establish individual profiles aiming at taking decision,
  - Data processing dealing with sensitive or social data,
  - Data processing having the purpose of surveillance (i.e. video surveillance),
  - Processing of children's data, national ID, biometric or genetic data,
  - Data processing concerning populations on a large scale,
  - Data processing with the purpose of protecting state security, or public safety should also be subject to a public assessment.

Some examples of assessment of categories of personal data processing presenting particular risks needing to be done at the level of EU: e heath records, smart grid

Final precisions.

- The European umbrella regulation on DPA provide for exclusion of the law the data processing operated by an individual for the purpose of his private and house life

- It provides for respecting the Freedom of expression of all, authors journalists, bloggers within the limits of freedom of speech concerning not

infringing the private life, the honour and reputation of individuals except in case of "public interest".

- It makes the link also with the need of balance with the need of Government transparency. In several member states the Data protection Supervisory authority is also in charge of the application of the law on access to public document.

- It also makes the link with the public national and EU statistics law and with the Archives law (which are open to the public, according to national laws, after a certain number of years depending where including personal data of the nature of the data -100 years for census information as an example- derogation for researches are also provided for under certain conditions regarding the publication of personal data)

Abstract

Which Urgent Initiatives to be Taken to Safeguard Our Freedoms with Regard the Current Worldwide Digital Developing Ecosystem

Marie Georges

Information and communication technologies are moving fast from a number of perspectives: local, regional, international in the field of ICT research, working division and use together with different methods of design (open source/proprietary), different economic models, huge competition

As the extension of use of ICT goes within our daily, frequent or exceptional activities whether collective or personal, more and more all of our different but interconnected freedoms and fundamental rights are at stake.

While it will be demonstrated that the general "Fair information practices", data protection", "data privacy "or" ICT and freedoms" principles, first established in the 70s, are still fully meaningful, the urgency is to evaluate up to which point our vision of the legal means to implement them, including at technical level, is still efficient or not, and if so which general common precisions or additions is now required. The gaps will be explored on each component of 'ICT and freedoms' laws (definitions/scope, basic safeguards /obligations of those designing, producing, or handling personal data, complementary safeguards /individual's rights, principles related to transfer of personal data to foreign countries, institutional means for implementation and enforcement, international cooperation).

Thegapswillbeillustratedbyconcreteexamplestakeninthosemarketingdesignatedareassu chas "blogs", "forum", "socialnetworks", "searchengine", "cloudcomputing", " bigdata", "internetofthings" andalsoinareasofgovernmentalpolicies (e health, electronic passport, digital fingerprints, DNA …)

The Edward Snowden's revelations, after those on Echelon in 2000/2001 and alerts done by US NGOs since 2009, place us this time in the urgency of evaluating, elaborating and implementing more precise rules, including on independent control, in the field of both targeted and "mass" secret surveillance in the interest of national security at national and on international level.

The speech will relay mostly on the European experiences, vision and current initiatives while taking into account the state of play of "Data Protection" in the world and other recent international initiatives in response to the E. Snowden revelations in particular at the Human rights Council of the United Nations.

최근 국제 디지털 생태계에서 자유를 보장하기 위해 어떤 긴급한 조치를 취할 것인가

Marie Georges*

목 차

사전 감사의 말

한국에서 제 경험과 생각들을 공유할 수 있게 초대해주어 감사하고 영광스럽다는 말을 건국대 법학전문대학원에 전하고 싶습니다. 2002년 이후 “ICT와 자유“의 법적 보호 시스템과 관련된 여러 주제에 관해 이번이 4번째 한국에 초대된 것이라 그 또한 뜻 깊은 일이라 할 수 있겠습니다. 국제적으로 “데이터 보호“ 또는 “데이터 프라이버시“라는 말이 좀 더 일반적이고 또 역사적으로 사용되고 있는 용어이기는 하지만, 제 관점에서는 앞으로 살펴볼 측면과 관련해 이 용어가 그렇게 정확한 용어는 아니라고 생각합니다.

*유럽, 프랑스 "ICT 및 인권" 분야 독립 전문가. "FREE Group" (유럽연합의 자유, 안보 및 정의와 관련된 주제에 관한 모니터링, 강의 및 옹호에 중점을 두고 있는 여러 유럽연합 국가의 Fundamental Rights European Expert Group 학자 및 전문가); DP 협약의 근대화 및 촉진을 위한 유럽 이사회 과학자 전임 프랑스 독립 "ICT 및 자유" 위원회(데이터 보호청) 자문 전임 유럽연합 집행위원회 내 1995년 DP 시행령 정교화 담당 분과 위원회 회원 국립 컴퓨터 공학 연구소(INRI) 학습 센터 경제학자. 그녀는 1973~1978년 프랑스에서 1978 DP법 채택을 옹호하기 위한 소규모 활동에 참가하였고, 이후 직원 조직 지원 및 여러 분야에 이 법을 적용하는 것을 지원하는 업무 담당으로 CNIL에 고용됨.

서론 - 도전과제, 기원, 효과적 솔루션을 위한 시급한 조치들

1. 정보통신 기술(ICT)는 여러 측면에서 빠르게 발전해가고 있다. 즉, ICT 연구 분야에서 지역적, 국제적 측면, 활동 분과 및 여러 상이한 설계 방법에 따른 용도(오픈 소스/독점 소스), 여러 상이한 경제 모델, 거대한 경쟁 등의 측면에서 빠르게 변화하고 있다.

우리의 일상생활, 업무, 취미, 관계, 일상적 또는 예외적 활동, 개인적 또는 집단적 활동에 있어 ICT의 사용 확대와 ICT 혁신[1]과 더불어, 서로 다르지만 상호 연관되어 있는 우리의 자유와 기본권, 집회의 자유, 정보의 자유, 종교의 자유, 자유롭게 이동할 수 있는 권리(위치 데이터) 등이 점점 더 많이 위험에 처하게 되었으며, 존엄과 저항의 권리도 위험에 처하게 되었다. 그 결과, 소위 "데이터 프라이버시 보호"는 점점 더 많이 실제 생활과 연관되어 있는 디지털 공간에서 우리의 모든 인권 행사를 지켜줄 기본적인 권리이자 수단이 되어가고 있다.

전문가로서 40년 동안 DP 분야에 종사해왔던 경험에 비추어 봤을 때, ICT와 관련해 서로 관련되어 있는 우리의 인권을 지키기 위한 구체적이고 바람직한 솔루션들은 "문화적 거리"와 관계없이 어느 곳에서나 매우 밀접한 관계를 지니고 있지만, 이를 구체적인 법적 제도 하에서 시행할 수 있는 가능성은 국가적, 국제적 차원의 정치적 협력과 함께 특정 시기의 정밀한 법적 제도와 비전에 달려 있다.

실제로, "공정한 정보 관행", "데이터 보호", "데이터 프라이버시" 또는 "ICT와 자유"라 불리는 일반적인 기본 원칙들은 1970년대[2]에 수립된 것들로서, 이러한 원칙들은 아직도 중요한 원칙들로 남아 있지만, 특정 시기의 특정 법적 제도 내에서 그러한 원칙들을 시행하는데 있어 가장 시급한 문제는 대부분 1990년대와 2000년대인 그러한 원칙들을 시행하기 위한 정밀한 법적 DP 제도가 기술적 수준을 포함해 정확히 어느 시점까지 효과적인지를 평가해보고, 그 결과에 따라 어떤 차이가 있는지 알아보고 그 차이를 메울 수 있는 방법을 찾아보는 것이다.

즉, 한 마디로 말하자면, 국경과 지역화, 글로벌화 내에서 발전하고 있는 IT와 서

1) 전문가에 따르면 현재 운영되고 있는 모든 IT는 10년 전에는 존재하지 않았던 것들이며, 나노 기술의 50%는 IT 분야에 속하게 될 것이라고 함.

2) 2013년 6월에 업데이트된 Bog Gellman의 FIP 의 미국 역사에 관한 웹사이트 http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. 참고
최초의 데이터 보호법은 EU 와 국제적으로 1970 년 독일의 Land Hessen 에서 채택되었고, 최고의 국가 DP 법은 스웨덴에서 1973 년에 채택되었으며, 프랑스의 « 정보 및 자유»법은 1978 년에 채택되었습니다. 국제적 차원에서 OECD DP 지침은 1980 년에 채택되었고, 유럽 협약 108 은 1981 년에 채택되었고, UN 의 DP 법 지침(CoE 협약과 더불어)은 1990 년에 유엔총회에서 만장일치로 결의되었으며, 108 협약으로 이어진 EU 의 시행령은 1995 년에 채택되었다

비스로 인해 급변하고 있는 세계에서 지속 가능한 데이터 프라이버시를 확보하기 위해서는, 정기적으로 IT와 서비스가 운영되고 있는 법적 틀을 평가해서 IT와 서비스가 인권을 효과적으로 보호할 수 있는 방향으로 진화해 갈 수 있게 하는 것이다.

2. 여러분과 오늘 그러한 차이를 확인하고 우리가 가지고 있는 모든 “ICT 및 자유“에 관한 법을 마케팅을 위해 개인 데이터를 처리하는 “블로그“, “포럼“, “소셜 네트워크“, “검색 엔진“, “클라우드 컴퓨팅“, “대용량 데이터“, “인터넷“ 등의 분야와 현재 처리되고 있는 매우 간섭적인 새로운 유형의 데이터나 새로운 유형의 처리 방식(디지털 지문, DNA, 얼굴 인식) 등의 분야, 그리고 e-정부 정책 분야(e 보건, 전자 여권, 디지털 지문, DNA 등)의 분야의 구체적인 예를 통해 그러한 법규를 구성하고 있는 여러 구성요소들을 살펴봄으로써(정의/범위, 개인 데이터의 설계, 생산 또는 취급에 있어서의 기본적인 보호장치/의무, 보완적인 보호장치/개인의 권리, 개인 데이터를 외국에 이전하는 것과 관련된 원칙, 집행, 국제적 협력을 위한 제도적으로 독립적인 수단 등) 그러한 차이와 가능한 솔루션을 파악하는 방법을 같이 나누고자 한다. 개인 데이터 처리의 폭발적 증가로 인해 지배 메커니즘을 평가하고 이를 보완하는 작업이 필요하게 되었다.

3. 개인 데이터 처리가 점점 더 국제화되고 있고, 여러 곳에 위치한 행위자들 간에 점점 더 많이 확산되고 있기 때문에, 즉, 사용자 장치(스마트폰/앱, 노트북/소프트웨어, 컴퓨터/소프트웨어)에서 네트워크(…) 수령자들의 장비를 통해 특정 목적의 개인 데이터 처리 용도로 클라우드 컴퓨팅 주체가 수령자들에게 제공하는 플랫폼으로 점점 더 많이 확산되고 있기 때문에, 다음과 같은 점들이 분명해지고 있다.

3.1. 데이터 처리 사슬을 구성하고 있는 각 구성요소들의 설계 및 시행은 데이터 보호 원칙을 관리함으로써 전체적인 데이터 처리에 기여해야 한다. 따라서 개인 데이터 처리 과정에 관련되어 있는 모든 당사자들에게는 일관적인 의무 조항이 적용되어야 한다.

3.2. 국가적 관점에서 봤을 때, 그러한 결과를 얻기 위해 현재는 수령국의 법적 틀에 대한 평가를 통해 잘 알려져 있는 EU의 “적절한 보호 원칙 수준“에 의해 채워지고 있거나 또는 필요한 경우 예외적인 보호조치를 취하는 것과 더불어 계약이나 강제적인 기업 규제를 통한 실용적 솔루션에 의해 채워지고 있는 자국 영토 밖에서도 유효한 법적 조치가 필요하며, 이를 통해 사용자/데이터 주체의 권리도 데이터와 함께 가야 한다.

4. Graham Greenleaf[3]에 따르면 전 세계적으로 DP 법을 채택하는 국가의 수가

3) 1970년대에는 8개국에 DP 법이 채택되었고, 1980년대에는 추가로 13개국이 DP법을 채택, 1990년대에는

증가하면서(지난달까지 101개 국가에 달함), DP법 간의 상충 또는 새로운 국가적 DP 법규와의 상충 현상이 발생할 수 있다.

다차원적인 맥락에서 그러한 갈등을 해소하기 위해서는 지배 메커니즘과 지배 메커니즘이 발전할 수 있게 만들 수 있는 수단을 포함해 국제적으로 구속력을 지닌 데이터 보호 수단 내에서 협력을 해야 할 필요성과 시급함이 제기된다. 이와 더불어, 두 지역의 조치는 실용적인 합의를 모색해야 하며(EU/APEC의 데이터 보호 당국), "상호 운용 가능한 법적 제도"라는 개념을 추구해야 한다(미국). 후자는 기술적 개념과 법적 개념을 기적적으로 혼합한 방식으로서, 이 방식은 일부 사람들에게는 정치적인 의문을 제기할 수도 있다.

현재 UN이 1990년에 구속력이 없는 "데이터 보호 지침"[4]을 총회에서 만장일치로 채택한 이후 그러한 방향으로 별다른 움직임을 보이고 있지 않는 상황에서 또한 NGO나 일부 정부의 최근 정치적 조치에 따라 UN이 마지못해 약간의 움직임을 보이는 상황에서는 합의에 이르는데 10~15년이 더 걸릴 수도 있으며, 아직까지는 마지막 근대화 작업이자 제 3국에 개방되었던 유럽회의에서 채택한 협약 108이 그러한 역할을 수행하고 있다. 이러한 비유럽국가의 지지는 아프리카 국가들(모로코는 이미 지지를 표명함)과 남미 국가들(우루과이는 이미 지지를 표명함)의 관심을 유발했던 것과 같이 아시아 국가들의 관심을 유발해 점점 더 많은 비유럽국가들이 새로 등장하고 있는 새로운 종류의 데이터 처리에 일관된 방식으로 이 법을 적용하는데 모든 당사자들과 협력하기 위해 옵저버(observer)로서 참가하길 원하고 있다. 이 근대화된 협약은 또한 세계 최초로 모든 관련국의 데이터 보호 당국이 여러 국가에서 처리되고 있는 개인 데이터에 관해 국제적인 불만이 있는 경우 법집행을 위해 세계 최초로 개인 데이터를 합법적으로 교환할 수 있게 해줄 것이다.

5. 우리에게 필요한 솔루션에 관한 이 강연 내용은 주로 현재 이미 데이터 보호가 헌법적 지위를 차지하고 있으며, 외국의 구글이나 페이스북과 같은 서비스에 관한 법적 조항을 갖고 있는 유럽의 경험에 기초하게 될 것이다. 1995년의 유럽의 데이터 보호 시행령은 2012년 2월부터 업데이트를 위한 검토 작업에 들어갔다. 집행목적으로 DP 규정과 다른 조항을 개정하자는 유럽연합 집행위원회의 제안에 대한 이 작업은 2014년에 종료될 것이며, 이 작업에는 유럽 의회에서의 4,000건 이상의 수정 사항이 포함될 것이며, 이 수정사항 중 대부분은 언론이 밝힌 바와 같이 경제 로비스타와 미국의 로비스트에 의해 영향을 받을 것이며, 미국과 EU의 NGO들로부

21개국이 추가되었고, 2000년대에는 35개국이 추가, 2000~2013년에는 24개국이 추가되어, 2013년 9월 현재 101개국이 DP 법규를 채택한 상태이며, 일부 국가는 모든 분야에 이 법을 적용하고 있고, 일부 국가는 민간 부문에만, 일부 국가는 공공 부문에만 이 법을 적용하고 있음. 참고문헌: Graham Greenleaf, Sheherezade andthe 101 Data privacy Laws, Origins, Significances and Global trajectories, September 2013 (http://papers.ssrn.com/sol3/papers.cfm?abstract id=2280877)

4) 1990년 12월 14일 총회에서 채택된 개인 데이터 파일의 규제 지침

터 비판을 받고 있는 사항들이다. 이러한 2개의 법규 전략은 특정 부문의 개인 데이터 처리에 있어서의 이해 균형상 필요한 경우(텔레콤 전화번호부에서의 전자 통신이나, 발신자 확인 등에 대해 해왔던 것과 같이) 특정 조항을 통해 보완을 하되 1개의 법규를 가지자고 주장하는 모든 유럽의 DP 전문가들이 찬성하지는 않는 전략이다. 하지만 현재의 유럽의 전략은 국가 연맹이 아니라 국가들의 연합이어서 특히 국가 안보 및 공공질서 부분에서는 유럽연합 차원에서 국가가 지니고 있는 모든 권한을 지니고 있지 못한 유럽연합의 특징에 기인한 것이라 할 수 있다.

DP에 관한 2가지 일반 법규라는 문제와 더불어 유럽연합에 관한 이러한 문제는 제 강연의 마지막 부분에서 다루게 될 범죄 예방이나 범죄 수사를 위한 경찰 서비스에 필요한 경우 민주주의 원칙에 맞게 사설 법인이 소유한 개인 데이터를 공개하는 것과 비밀 정보국에 의해 부분적으로 운영되고 있는 국가안보를 위해 경찰이 수집한 데이터를 공개하는 문제에 관해 민주사회에서의 DP 원칙의 제약 또는 예외사항에 관한 문제를 제외하고, 더 이상 구체적으로 다루지는 않겠다.

2000/2001년의 에셜론(Echelon) 공개 및 2005년과 2008년 NSA와 PRISM에 관한 미국 NGO의 경고 이후 Edward Snowden의 정보 공개는 법적 민주적 원칙과 통제 수준을 수립하는 것에 있어 당시 구체적인 긍정적 효과는 거두지 못한 채 문화적, 경제적 지배를 위해 인프라를 관리한다는 미명하에(ICANNN과 재정적 천국을 사용하고 있는 미국의 전 세계 기관들이 차지하고 있는 장소의 수가 증가하고 있는 점을 보라) 자행되고 있는 거대한 반역에 직면하는 것을 예방하는 것은 말할 것도 없이 그러한 비극적인 거대한 자유의 상실을 막기 위해 정치적, 법적인 조치를 취해야 할 긴급한 상황에 처하게 만들었다.

6. 그 결과 DP 법에 관한 우리의 모델과 세계적인 DP 규정을 개정해야 할 필요성과 본 발표에서는 다루지 않았지만 그러한 지배에 맞서 이 디지털 공간에서 우리의 자유를 지키기 위해 또 다른 성격의 조치들을 취해야 할 필요성이 제기되었다.

- 정치적인 측면에서 민주사회에서 시민에 대한 감시를 금지하고 있는 것과 마찬가지로, 우리는 전세계적 차원에서 자국의 경제적, 산업적, 정치적 이득을 위해 해당 국가의 기관들을 통해 어떤 수단을 통해서라도 타국의 활동을 감시하는 것을 금지하는 것을 합의해야 한다.
- 기술적 지배 측면에서 우리는 아직도 미국 정부와 연관되어 있는 ICANN 대신 유엔의 통제를 받는 복수 이해관계자들로 구성된 진정한 세계적 지배구조를 모색해야 한다.
- 산업적 측면에서 우리는 다음을 통해 그러한 스파이 활동과 지배를 방지할 수 있는 수단을 강구해야 한다.
- 국가적 또는 지역적 “클라우드 컴퓨팅 서비스“ 및
- 비밀유지 기법.

Ⅰ. IT의 진화와 IT 사용에 관한 90년대와 2000년대의 비전에 기초한 DP 법적 제도의 구성 요소에 대한 평가

1. ICT와 데이터 보호의 기본 원칙 간의 관련성

"데이터 보호"의 목적은 무엇인가?: 데이터 보호의 목적은 해당 개인의 성격 또는 ID를 담고 있는 개인 데이터는 "전용"의 대상이 아니라는 점과 이러한 보호는 개인의 보호와 직접적인 관련성이 있다는 점을 염두에 두고 개인 데이터를 타인(고용주, 상업적 집단, 은행, 공공 기관, 자선단체, 정치적 정당 등)이 남용하는 것을 방지하기 위한 것이다.

남용 가능성은 심지어 해당 개인이 알지 못하는 사이에 디지털화된 개인 데이터가 쉽게 그리고 저비용으로 수집될 수 있으며(예: 비디오 감시), 장시간 보관될 수 있고(잊을 권리에 기초해 "오프라인" 세상에 있어 법적 조항이 존재하기는 하지만), 재사용될 수 있으며(예: 이익이나 기타 용도로), 조작/변경될 수 있고, 다른 디지털화된 소스와 매치될 수 있고(공통 식별자 또는 고유 식별자 또는 여러 파일에 있는 동일 데이터 세트에 기초해 정교화된 프로파일에 기초해 상업, 경찰 또는 사법 분야에서 해당 개인에 결정을 내리는 경우), 더 적은 비용으로 멀리 떨어져 있는 곳에서 이 데이터를 처리할 수도 있고, 심지어 고의이든 비 고의이든 공개될 수 있으며, 오조작에 의해 삭제 또는 손실될 수도 있다는 점에 기인한다.

따라서 지금까지 계속 정교화되고 있는 DP 원칙들은 처리 조작의 설계 단계와 시행 단계 둘 모두에서 개인 데이터의 처리 설계를 규제함으로써 그러한 남용을 예방하는 것을 목표로 하고 있다.

- 이를 위해 개인 데이터에 대한 정의, 규칙으로 고려할 원칙 리스트의 설정 및 이를 어떻게 적용할 것인지를 정해야 할 필요가 있다.

2. 정의 또는 해석과 관련된 주요 차이들과 가능한 솔루션

개인 데이터는 "확인 가능한 개인과 관계된" (협약 108), "식별 번호나 물리적, 정신적, 경제적, 문화적 정체성과 관련된 여러 요인들을 참고해 직접 또는 간접적으로" 누구든 신원을 확인할 수 있는("데이터 주체"에 대한 95 EU 시행령의 정의) 데이터로서, 로비스트의 관점에서 "합법적이든 아니든 신원을 확인할 수 있는" 데이터라는 정의가 어렵게 해석되는 데이터이다.

- 따라서 개인의 이름이 없는 개인과 관련된 “원“ 데이터라도 그 내용에 따라 그 개인을 식별할 수 있다. 통계학자들에 의해 어떤 사람의 직업, 성별, 연령 및 위치로 그 개인을 알 수 있다는 사실이 잘 알려져 있다. 이는 과거 특정 조건을 부여하지 않고 제 3자가 연구 목적으로 익명화한 데이터에 관해 얘기할 때 중요한 문제이었다.
- 과학자들이 밝혔던 바와 같이 이는 처리 데이터가 폭발적으로 증가함에 따라 더 이상 유효하지 않게 되었다. 한 사람의 이름이나 “사회학적 데이터“ 없이 그 사람에 대한 개인 데이터를 더 많이 가지면 가질수록, 그리고 더 많이 발표되면 될수록 그 개인을 더 쉽게 식별할 수 있을 것이다.

- 현재 유럽 의회의 일부 사람들은 “익명 데이터“를 정의하는 문제를 피하고 싶어 하기 때문에 익명 데이터를 정의하는 것을 피하는 것이 더욱 중요하다.
- 어떤 사람들은 데이터 사용에만 초점을 두고 개인으로부터 데이터를 수집하는 단계는 신경 쓰지 않으려 하지만, 우리는 모든 DP 원칙을 데이터 수집단계에서부터 사용단계에 이르는 모든 단계에 적용할 수 있는 방법을 찾아야 한다. 이는 통계적 목적으로 사용되어 규정의 적용을 받지 않는 “익명“ 데이터로 알려진 “대용량 데이터“에 있어서도 중요할 수 있다. 최소한 이러한 맥락에서 세계적으로 대량으로 사용되고 있는 서비스는 그러한 측면에서 발표되는 숨은 통계치를 정교화하는 것을 허용하거나 공공 이익을 추구하기 위한 민주적 통제를 받지 않는 일이 없도록 해야 한다(이에 대해서는 아직 특별한 조치가 없음).

온라인 환경은 또한 개인의 IP 주소를 제외하고 실시간으로 개인과 관련된 어떤 내용도 알지 못해도 그 개인에 영향을 미칠 수 있는 상호작용이 가능하게 만들고 있다. 이는 EU의 DPA 당국이 EU 의회에서의 DP 패키지에 대한 MP의 보고서에 따라 개인의 식별을 배제할 수 있게 만든 것이다. 이는 법률적 근거 없이 EU의 개인 데이터 정의에 추가될 정밀성이라 할 수 있다.

프로파일링: 그러한 기법을 더 많이 사용할수록 이미 95 EU 시행령에 포함되어 있는 관련 보호조치의 정의를 더 정밀하게 만드는 결과를 낳게 된다. 여기서 EU는 유럽회의의 협약 108에서 정교화한 정의를 취하고 있는데, 그 정의는 “자연인의 개인적 측면을 평가할 용도 또는 특히 자연인의 직무 성과, 경제상황, 위치, 건강, 개인 선호, 신뢰성이나 행동을 분석 또는 예측하기 위해 개인 데이터를 자동으로 처리하는 모든 형태“이다.

제품: 개인 데이터 처리의 “통제자(controller)“ (데이터 제작을 결정하는 사람)와 통제자를 대신해 행동하는 제 3자인 “처리자(processor)“의 정의에 더해 서론에서 언급했던 필요성과 함께 DP 원칙을 개인 데이터 처리 설계 및 운영 사슬에 관여하

고 있는 모든 당사자들에게 적용하기 위해 EU 의회에서 MP 보고서에서는 다음과 같은 “제작자(producer)“의 정의를 제안하였다: ’제작자’는 자연인 또는 법인, 공공 당국, 기관 또는 데이터 통제자가 개인 데이터를 처리할 목적으로 설계된 자동화된 데이터 처리 시스템 또는 파일링시스템을 제작하는 기타 기구“. 이 정의를 이용자가 채택하기를 희망한다.

3. 리스트가 잘 알려져 있는 상호 연관된 DP 원칙은 더 높은 강도로 효과적으로 적용되어야 한다.

- 특히 데이터를 불공정하게 수집하는 것을 허용하지 않는 것을 의미하는 공정하고 합법적인 데이터 수집 및 처리 원칙. 합법적으로 운영되고 있는 비디오 카메라는 개인에게 카메라가 운용되고 있다는 사실을 개인에게 얼마나 잘 알려주며, 데이터 주체에게 즉시 제공되어야 할 확장 정보를 개인에게 얼마나 잘 제공하는지를 볼 것.

- 데이터의 잠재적 재사용과 이 데이터를 사용할 데이터 수령인에 관한 원칙을 포함해 구체적이며, 명시적이고 합법적인 용도의 원칙
  처리의 용도에 관한 합법성 또는 법적 기초 분야에 있어 현재까지 기본적인 데이터 처리 보호장치, “해당 개인의 동의“라는 문제는 “계약 이행에 필요한 것“이나 “법적 의무 이행에 필요한 것“ 또는 “공공 기관에 부여된 업무를 이행하기 위해 필요한 것“과 같이 다른 모든 법적 기초와 관련된 대부분의 구체적 상황에서 다소 이론적인 차원의 문제였지만, 특히 어떤 서비스를 제공하는 과정에서 수집된 데이터를 다른 목적의 서비스에 사용할 가능성이 높은 온라인 서비스를 제공하는 기업체와 관련해 개인의 동의는 점점 더 중요해지고 있는 문제이다.
  데이터 수집의 원래 목적과 다른 용도라는 상황을 피하기 위해, EU 집행위원회는 대부분의 전문가와 NGO의 견해와 일치하는 견해를 보이고 있는데, 이 견해는 제 관점에서 봤을 때는 유럽의회가 채택할 것으로 보이며, 현재로서는 동의에 관한 보다 정밀한 정의가 필요한 실정이다. 현재의 정의에 따르면 동의는 구체적이며, 내용을 알려준 뒤에 받아야 하며, 자유로워야 하면서 동시에 데이터 주체의 긍정적 행동을 통해 명시적인 성격의 것이어야 한다.

- “최소화 원칙“이라고도 불리는 적절하면서도 관련성이 있고 비례적인 원칙은 사용되는 데이터의 성격/수량 및 합법적 용도에 따른 보유 시기 둘 모두에 적용되는 원칙이다.
  이 원칙은 이동할 권리에 있어 데이터의 보유 기간이나 정보 및 자신의 생각에 대한 권리에 있어 검색 엔진에 요청하는 것과 같은 경우에 점점 더 중요

한 역할을 담당하고 있다. 이 보유 기간은 기본적으로 0 근처이어야 하며, 기간이 더 긴 경우는 사용자의 자유롭고 명시적인 동의에 기초하거나 범죄 가능성을 방지할 목적 또는 중대 범죄에 대한 수사 목적인 경우에 국한되어야 한다 (후자의 경우는 사이버범죄에 관한 부다페스트 협약에서 정한 3개월). 후자의 경우, 구체적인 EU 시행령이 정하고 있지만 각 회원국의 결정에 달려있는 모든 사용자 트래픽 데이터(traffic data)의 6~24개월의 보유기간에 대해서는 EU의 여러 헌법재판소에서 수정이 요청되고 있다. 안타깝게도 아직 우리는 이 규정의 개정을 기다리고 있는 상황이다.

- "민감 데이터"가 위험할 경우 보호 강화

  동의 없이 처리가 금지된 데이터 리스트(법이 데이터 주체의 보호 동의에 따라 사용을 금지한 경우에도) 또는 특정 안전장치를 제공하고 있는 법의 기본이 EU에서의 유전자 데이터 및 개인에게 고유한 생체인식 정보에 대한 최신 유럽의회 협약에도 확장될 것으로 예상된다. 원래의 리스트는 데이터를 사용하면 차별의 위험성이 있는 데이터에만 적용되어 작성되었다. 즉, 인종이나 정치적 의견, 종교, 무역단체의 소속, 건강, 성 생활 및 처벌 등에 관한 데이터, 또는 보안 조치 등에 대한 데이터 등에만 적용되어 작성되었다.
  이 주제에 대해서는 유럽에 대해 많은 사실을 알아야 한다. 그 예로는,

  - 생체 인식 데이터 및 유전적 데이터 : 프랑스의 헌법위원회는 EU 여권이나 동일한 성격의 국가 ID를 취득하기 위해 관련 파일에서의 2개의 디지털 지문 및 RFID에서 2개의 보호 디지털 지문 대신 10개의 지문을 보유하는 것을 기각했습니다. 관련법에 대해 헌법 위원회에 제소한 70 MP들의 주장 또한 그러한 파일이 민주적 국가의 붕괴나 침략 상황에서 저항할 권리와 관련해 모든 국민들을 위험에 노출시킬 수 있다는 것이었다. 독일 의회는 2005년에 EU 여권을 일단 독일인에게 발행한 경우, 어떤 디지털 지문도 파일에 보관할 수 없는 것으로 판결했다. 스트라스보르그 유럽 인권 법원은 2008년 영국에 대한 판결에서 법원이 유죄가 아닌 것으로 판결한 개인과 관련된 경찰 파일에 유전자 데이터와 디지털 지문을 보관하는 것이 무죄추정의 원칙에 반하지 않는다고 판결하였다.
  - 건강 데이터: 프랑스에서 웹 사이트를 통해 건강 데이터를 제 3자에게 공개하는 것은 해당 개인의 동의가 있다 하더라도 법으로 금지되어 있다.

- 전자 전송의 경우를 포함해 처리되는 개인 데이터와 소프트웨어에 적용되는 보안 원칙은 여러 유럽 국가 및 미국에서 중요한 사건들이 여러 차례 발생해 그 필요성이 제기된 이후, 보안 위반이 있을 경우 이를 관할 DPA에 통지해야 하는 의무조항으로 보완했다.

- 개인이 자신의 데이터가 어디에 어떻게 사용되는지를 알고 이를 통제할 수 있는 권리의 형태로 개인을 보호하기 위한 보완적 보호 장치

이는 전통적으로 다음과 같은 여러 가지 권리를 통해 시행되고 있다.

o 데이터 통제자가 데이터 수집 시에 데이터 주체에게 제공하는 해당 정보
이 정보는 통제자의 이름과 주소, 데이터 수집의 목적, 제공해주는 정보, 수령인을 넘어 보유 기간과 EU외부로의 데이터 이전 가능성과 그러한 권리를 행사할 수 있는 사용자 친화적인 수단과 즉시 제공해야 한다는 조건으로 확대될 것으로 보인다(URL 뒤에 숨겨져 있지 않아야 함).

o 처리/보관된 자신의 데이터에 접근할 권리와 이 데이터가 불완전하거나 오류가 있거나 비합법적인 데이터인 경우 이 데이터를 수정할 권리

2개의 보다 정밀한 내용이 추가될 것으로 예상된다.

"이동성의 권리"는 표준화된 형식으로 자신의 데이터를 온라인에서 얻을 수 있는 권리(자신의 개인 데이터 처리에 유용하거나 한 서비스 제공업체에서 다른 제공업체로 옮길 때 유용한 경우) 그리고,

"잊혀질 권리"는 억제의 권리(right of suppression)를 정교화한 것이다(발표 데이터 및 검색 엔진에서 검색할 수 없는 데이터 분야).

o 프로파일링 기법을 사용할 때 자동 의사결정의 위험성에 관해, 1978년 이후 필요한 것으로 보이며 EU 95 시행령에서 규정한 추론을 반박하고 최종 판결 전에 정보를 추가할 권리에 관한 특정 보호 장치(또한 그러한 처리에 기초한 자동 의사결정은 사법적 판결 분야에서 절대적으로 금지되어야 함).

o 마케팅 용도로 데이터의 재사용이 지니는 경제적 이점에 관한 것으로서, 이미 EU의 프라이버시 시행령에서 사용 기법의 간섭 정도에 따라 이해 균형이 일부 맞추어져 있다 : 전화나 전자 통신을 통해 해당 개인의 명시적 동의가 필요한 경우 용도를 알릴 의무 및 그러한 용도를 거부할 권리(미국의 'opt out' 권리와는 다른 "반대할 권리"로서 해당 개인에게 알릴 의무를 포함하지 않음)

o 우리는 일부 EU 회원국에 있어 결코 공개될 수 없는 범죄 기록(EU 범위 밖에서)의 경우, 해당 개인이 자신의 모든 기록에 접근할 수 있는 권리는 법에 의해 해당 정보를 얻을 권한이 없는 타인으로부터의 압력에 맞서 해당 개인을 보호하기 위한 경우에만 이 정보를 참고할 수 있게 제한하고 있다.

o 데이터 보호 감시 당국이나 개인이 선택한 법원에 이의를 제기할 권리
이 권리는 개별적으로 주어지는 권리이지만, 개정된 EU 규정 내에서는 인권관련 NGO를 통한 집단적 이의제기나 집단소송제도를 통해서도 이의

제기를 할 수 있게 될 것으로 예상된다.

II. 실질적 원칙("민주사회에서 필요하다면")의 한계와 관련된 조항의 평가

- 본 강연에서는 중요한 공공의 이익에 대한 제약 또는 기타 권리의 보전이라는 목표들과 관련된 자세한 내용을 다루지는 않을 것이다.
여기서는 국가 안보의 제약에 관해서만 언급하도록 하겠다.

- 국가 안보와 같은 분야는 국내의 모든 사법적 가능성을 거친 이후 개인이 이의를 제기할 수 있는 유럽 인권 법원(스트라스보르그)이 관할하는 문제이다. 법학적으로 그러한 제약을 위한 법률은 명료하고 정확해야 한다.
그러한 법률은 다음과 같은 사항을 제시해야 한다.
수정사항을 정당화 할 수 있는 사항들
독립적 기구의 승인 절차(긴급상황 시는 제외)
비밀 감시의 경우 그러한 감시의 기간, 새로운 승인을 받은 감시의 범위
해당 독립적 기구에 의한 사후 관리(독립적 기구의 회원은 제 견해로는 정부가 아닌 의회에서 임명해야 한다고 본다)
대중들을 위한 투명한 활동 수단: 담당 기관이 요청한 각 목표 별 승인 사건 및 미 승인 사건 수, 관리의 결과 등
또한 그러한 감시는 사법 절차와는 완전히 독립적인 방식으로 운영되어야 한다.

제 의견으로는 이러한 정밀함이 협약 108의 EU 데이터 보호 조항에 추가되어야 할 수 있을 것이며, EU는 이 협약과 인권 법원(총 48개국 중 EU는 유럽의회 소속의 28개국이 가입)을 설립한 유럽의회의 인권 협약을 준수해야 할 것이다.

국제적인 차원

III - 데이터를 외국(또는 EU에서 제 3국으로 또는 협약 108의 회원국이 아닌 국가)으로 이전하는 것에 적용되는 규정의 예상 업데이트에 대한 평가

- 개인 데이터의 유통을 승인하는 원칙으로서 외국 DP 수준의 적절성을 판단하기 위해서는 해당 국가에 관한 유럽의 인정이 필요하다.

이 솔루션은 해당 개인에게 공정한 솔루션인데, 그 이유는 개인의 권리가 개인의 데이터와 함께 존재할 수 있기 때문이다.

- 하지만 현재 많은 발전을 보이고는 있으며 과거의 국가적 경험, 특히 프랑스의 경험을 바탕으로 EU에서는 실용적인 수단을 강구해오고 있기는 하지만, 세계의 모든 국가들이 안타깝게도 아직 그러한 보호를 제공하고 있는 것은 아니다.

그러한 실용적인 솔루션은 2가지 종류로 볼 수 있다.

- 계약적 솔루션은 데이터 통제자 간 또는 데이터 통제자와 처리자 간의 관계에서 유럽의 모든 국가들이 사용하고 있는 수단입니다. EU차원에서 계약 모델이 수립되어 있다.
- 다른 솔루션은 기업이나 기업의 계열사들이 자체적으로 일방적인 선포를 하는 것이다. 우리는 이러한 수단을 구속력이 있는 기업 규칙이라고 부른다. 해당 DPA의 승인을 받아야 하는 이러한 수단의 내용과 절차의 모델을 EU DPA 실무자들이 정교하게 만들어 놓았다.

  하지만 몇몇 회원국들은 그러한 일방적 선포의 법적 지위를 인정하지 않을 수도 있다. 이 수단은 유용한 것으로 입증되고 있기 때문에(하지만 절차가 너무 오래 걸리는 것으로 나타남), 유럽집행위원회는 구속력이 있는 기업 규정을 개정 DP 조항에서는 절차를 간소화 하는 조건 하에 이 규정에 법적 지위를 부여할 것을 제안하고 있다.

이러한 접근 방식은 다음과 같은 여러 가기 사항에 기초한 “적절한“ 보호의 원칙의 수정을 포함하고 있다.

- 해당 개인의 동의 , 또는
- 데이터 이전이 물리적, 법적으로 동의를 해줄 수 없는 상황에 처한 개인의 중요한 이익을 보호하기 위해 필요한 경우

  제 견해로는 동의에 의한 수정은 반복적인 이전이라는 기초가 아니라 특별한 이전의 경우에만 이루어져야 하고, 해당 개인에게 DP 보호를 보장할 수 없다는 사실을 알려주어야 한다고 생각한다.

또한 다음과 같은 사항에 기초한 원칙의 수정도 제안되었다.

- 공공 이익이라는 중요한 근거, 또는
- 법적 주장의 제기, 행사 또는 방어를 위해

또한 소송을 준비하는 몇몇 절차에서는 유럽에 있는 계열사가 미국과 이메일이나 파일을 교환할 수 있게 할 것을 요구하고 있다는 것이 발견되었다. 또한 미국의 기관이 요청했을 때 계열사 직원이 미국과 관련이 없는 애국자법(Patriot Act)에 해당되는 데이터를 해외로 제공하는 것과 관련된 위험성도 발견되었다. 여러 사례에서

그러한 계열사의 법률 자문가들은 그러한 데이터 제공이 허용되는지의 여부를 알기 위해 DPA에 연락을 하기도 했다. DPA는 해당 사례의 구체적 내용을 알려달라고 요청했으며, 상호 지원 조약에 규정된 절차에 따를 것을 조언해주었다. 이것이 2011년 11월 버전에서 제안된 규정에 데이터 통제자 또는 처리자가 DPA에 통지해야 하는 의무 조항을 포함시킨 이유이며, 이러한 통지에 따라 DPA는 해당 데이터의 공개를 승인하고 해당 기관에 이 사실을 알리고, 데이터 통제자나 처리자는 해당 개인에게 데이터 이전이 승인되었음을 알리도록 하였다.

놀랍게도 이 제안은 2개월 후에 공개된 유럽연합 집행위원회의 제안에서는 빠져 있었다.

Edward Snowden이 지난 6월에 공개하였고 가디언지와 뉴욕 타임지에 실린 PRISM이 제기한 국제법 위반 사례, 즉 유럽에서 운영되고 있는 미국 기업으로부터 데이터를 얻기 위해 애국자법을 사용하고 있다는 사실의 공개로 인해, 이 사건이 일어나기 전에 제안되었던 사라진 조항은 유럽의회가 채택한 본문에 다시 등장하게 될 것으로 보인다.

현재 PRISM 스캔들로 인해 독일 DPA 컨퍼런스에서는 개인 데이터를 미국에 이전하는 것을 승인하지 않기로 결정했다.

유럽의회는 또한 다음과 같은 사항을 유예 가능성을 탐색하고 있다.

- “안전 항구(safe harbor)“라 불리는 미국 내 상업 부문에서의 적절성에 대한 EC의 결정
- 항공기 예약과 출발 72시간 전에 미국 당국에 모든 예약사항(미국이 저장하기를 원하는 내용과 시간이 과도한 것으로 DPA들이 생각하고 있는 데이터 포함)을 보내야 하는 항공사에 관한 PNR 협정
- 특정 조건에서 Swift에 의해 시행되고 있는 벨기에에 기반을 두고 있고 특히 미국에 계열사를 두고 있는 회사의 재무 데이터를 미국에 이전하는 것에 관한 Swift 협정. 이 협정은 워싱턴 포스트지가 2004년 미국 정부가 미국과 관련되어 있지 않지만 미국 내 Swift 계열사에 기초해 시스템에 백업으로 접근하고 있는 데이터를 폭로한 이후에 체결된 협정입니다. 동시에 Swift는 유럽에도 백업 데이터를 전송하기로 결정되었다.

유럽의회의 자유, 안보 및 사법 위원회의 조사와 추천사항에 관한 보고서는 12월에 작성이 완료되어 2014년에 시작되는 유럽의회 정기총회에서 논의될 것이다.

IV. 실질적 원칙을 효과적으로 적용하기 위한 수단

그러한 수단들에 대한 EU의 평가는 현재까지는 주로 다음과 같은 사항에 중점을 두고 있으며,

- 데이터 보호 감독 기관의 권한(독립적, 사전 및 사후 수사 권한)
- 제재 (벌금, 처벌)
- 구제

이러한 평가는 주로 데이터 처리 및 불만의 폭발적 증가로 인한 데이터 통제자, 처리자 및 데이터 보호 감독 기관의 변화와 보다 일반적인 시행 방안 및 규정에 대한 필요로 표현되는 EU 차원의 변화로 이어질 것으로 예상되고 있다.

- 원칙을 존중하기 위해 공공 부문 및 민간 부문의 데이터 생산자, 통제자, 처리자 들은 다음 사항에 관한 독립적 지위를 보장해주는 프라이버시 담당자를 임명할 것으로 예상되고 있다.
  - o 직원 교육
  - o 그 리스트가 DPA의 제안에 기초한 유럽의 일관성 메커니즘 내에 제시되어 있는 프라이버시 침해의 위험성이 있는 데이터 처리에 대한 명시적 평가의 정교화
  - o 처음부터 프라이버시를 염두에 둔 개인 데이터 처리의 설계와 기본적인 설계 및 개인 데이터 처리의 시행
  - o 모든 데이터 처리의 자체 기록 및 업데이트
  - o 책임자나 필요한 경우 DPA에 통지
  - o 권리 행사 요구 및 불만사항에 대한 대응

- DPA는 다음과 같은 “전통적인 업무“외에도,
  - o 인식
  - o 자문 및 추천사항 ,
  - o 전문 규정의 검토 ,
  - o 불만사항에 따른 또는 자체적 판단에 따른 수사(DPA에 정보를 제공하는 비밀보장의 의무가 있는 사람에 대한 보호 및 DPA 회원 및 직원의 비밀 유지 의무 수립)
  - o 새로운 IT 또는 활동의 감시
  - o 법안이나 규정안에 의견 제시 ,
  - o 활동의 투명성 보장
  - o 필요한 경우 대중적 논쟁에 기여하고, 국가나 기관장에 추천사항 제시

  다음과 같은 사항이 추가될 것으로 예상된다.

o 공공 또는 민간 기구로부터 개인 데이터 처리에 관해 통지 받은 사항을 더 이상 등록할 필요가 없음

o 하지만 사전 통제를 실시하는 대신 프라이버시 침해 위험성이 있는 데이터 처리에 대한 통제자의 평가를 검토하는 것

o 인증서 발행(추후 더 세부적으로 수립될 절차)

o 기업의 연간 매출액의 최대 2%까지 벌금을 부과하는 것. 이러한 벌금 수준은 기업을 배려한 벌금 수준으로서, EU 국가에서는 이 보다 더 높은 벌금을 부과하고 있으며, 이미 그러한 제재 권한을 지닌 DPA들은 현재 주로 개인 데이터를 자원으로 전 세계적으로 서비스를 제공하는 기업들의 엄청난 위반 행위를 고려할 때 그러한 벌금 수위는 충분하지 않은 것으로 판단하고 있으며, 5% 정도가 적절한 수준이라고 판단하고 있음.

예시: 구글의 스트리트뷰. 구글은 비밀리에 커뮤니케이션 데이터를 수집하고 있으며, 거리를 찍어 서비스로 제공하고 있다. 일부 DPA는 이미 제재 권한을 갖고 있지만 통상적인 최대 벌금 한도의 권한을 지니고 있다. 이 DPA들이 부과할 수 있었던 제재조치는 2011년 프랑스의 경우 10만 유로, 독일의 경우 14만 5천 유로에 불과했습니다. 미국에서는 2013년 동일한 위반행위에 대해 7백만 달러의 벌금을 부과했다.

o EU 내 국가 간 데이터의 유통과 관련해 아직도 본부 소재지의 관할 DPA가 감독이 책임을 지고(유럽연합 집행위원회의 의견), 데이터 처리에 관한 실제 판결이 이루어지는 장소, 해당 지역에 통제가 필요한 위치, 국가적 성격을 지니고 있어 EU 회원국 마다 다른 특정 데이터 처리를 규정한 법적 기, 해당 개인의 이익 등에 따라 다른 DPA의 협력을 구할 것인지(EU DPA의 실무자 및 여러 전문가의 의견)를 결정하는 일이 남아 있다.

이러한 논의 외에도 일부 전문가들은 규정을 위반한 국경을 넘은 데이터 처리에 대해 EU 차원에서 각국의 DPA와 유럽 DP 감독국(EDPS), EU 기구의 데이터 처리 감독 당국 등으로 구성된 유럽 데이터 보호 위원회가 제재 수위를 결정할 필요가 있다는 점을 부각시키고 있다.

- 유럽 데이터 보호 위원회 (예: “EU DPA 실무자)는 규제 차원에서 일관성 메커니즘을 담당함으로써 더 강력한 역할을 담당하게 될 것이다 (특히 특정 위험성을 내포한 데이터 처리 리스트에 대한 국가 DPA 제안에 대한 판단, 부문에 관한 추천사항, 유럽연합 집행위원회의 제안에 의견 제시 등). 유럽 데이터 보호 위원회 사무국은 더 이상 유럽연합 집행위원회의 구조가 아니라 유럽 DP 감독국(European DP Supervisor) 산하에 속하는 기관이 될 것이다.

- DP 평가 절차의 대상이 되어야 하는 특정 위험을 내포한 데이터 처리에 관한 최초의 리스트
- 의사결정을 내리기 위한 목적의 개인 프로파일을 만들기 위한 데이터 처리
- 민감한 데이터나 사회적 데이터를 다루는 데이터 처리

- 감시 목적의 데이터 처리(예: 비디오 감시)
- 아동 데이터, 국가 ID, 생체 인식 또는 유전자 데이터의 처리
- 인구에 관련된 대규모 데이터의 처리
- 국가 안보 보호 또는 공공 안전을 위한 데이터 처리는 공공 평가의 대상이 되어야 한다.

EU 차원에서 실시될 필요가 있는 특정 위험을 내포한 개인 데이터 처리의 범주별 평가 예: e 보건 기록, 스마트 그리드

최종 정밀성

- 유럽의 DPA에 관한 포괄적 규정은 개인의 사적인 생활을 위해 개인이 운영하는 데이터 처리는 법 규정에서 제외하고 있다.
- 이 규정은 개인의 생활, 명예, 평판을 침해하지 않는 범위 내에서 공공의 이익을 위한 경우를 제외하고 모든 저자, 기자 및 블로거들의 언론의 자유를 존중하고 있다.
- 이 규정은 또한 정부의 투명성에 대한 필요성과의 균형과도 연관되어 있다. 몇몇 회원국의 경우, 데이터 보호 감독 기관이 공공 문서에 대한 접근에 법을 적용하는 문제를 담당하고 있다.
- 이 규정은 또한 국가 및 EU 통계법 및 기록물 법(개인 데이터를 포함해 몇 년이 지나면 일반에게 공개되는 기록물-예를 들면 인구조사 데이터는 100년 후 공개, 개인 데이터 발표에 관한 특정 조건에서는 연구 데이터도 공개될 수 있음)과도 연관이 있다.

국문초록

최근 국제 디지털 생태계에서 자유를 보장하기 위해 어떤 긴급한 조치를 취할 것인가

Marie Georges

IT 기술은 다방면에 걸쳐 빠르게 발전하고 있다. 즉, 상이한 설계 방법(오픈 소스/독점 소스), 서로 다른 경제 모델, 다량의 소비 등과 함께 지방, 지역 및 국제 ICT 연구 분야, 업무 분과 및 용도 등의 측면에 있어 빠르게 발전하고 있다.

ICT 활용이 집단적이든 개인적이든 우리의 일상적인 활동 또는 예외적 활동으로 확대되고 있음에 따라, 서로 다르지만 상호 연결되어 있는 우리의 자유와 기본권이 위험을 받고 있는 상황이 되었다.

70년대에 처음 수립된 일반적인 "공정한 정보 활동", "데이터 보호", "데이터 프라이버시" 또는 "ICT 및 자유에 관한 원칙들이 아직도 중요한 역할을 하고 있지만, 기술적인 수준을 포함해 그러한 원칙을 시행에 옮길 우리의 법적 수단에 관한 비전이 어디까지 효과적인지를 평가하는 것이 시급한 일이면, 만일 그렇다면 어떤 정밀함과 추가 사항이 필요한지를 평가할 필요가 있다. 그 차이는 'ICT 및 자유에 관한 법'의 각 구성요소(정의/범위, 그러한 디자인의 안전장치/의무사항, 개인 데이터의 작성 또는 취급, 개인 데이터를 외국으로 이전하는 것과 관련된 보충적인 안전장치/개인의 권리, 원칙, 시행 및 집행을 위한 제도적 수단, 국제적 협력) 별로 살펴볼 것이다.

그 차이는 '블로그', '포럼', '소셜 네트워크', '검색 엔진', '클라우드 컴퓨팅", '거대 데이터', '인터넷' 등과 같은 지정된 마케팅 분야에서 구체적인 예를 통해 살펴볼 것이며, 또한 정부 정책 분야에서의 예를 통해서도 살펴볼 것이다(e 보건, 전자 여권, 디지털 지문, DNA….).

2000/2001년의 Echelon과 2009년 이후 미국의 NGO 들이 제시한 경고 이후 Edward Snowden이 드러낸 사실들은 국가 및 국제 수준에서 국가 안보를 위한 대상 및 집단적인 비밀 감시에 대한 독립적 통제를 포함해 보다 정밀한 법규를 평가하고, 정교화하며 시행하는 것이 시급하다는 사실을 보여주고 있다.

이 발표는 대부분 유럽에서의 경험과 비전, 현재의 활동 등에 초점을 둘 것이며, 이와 동시에 E. Snowden의 공개에 대한 대응, 특히 유엔의 인권위원회에서의 세계 및 기타 최근의 국제적 활동에 있어서의 “데이터 보호”의 현황도 고려할 것이다.

제4주제

빅데이터와 프라이버시, 공정경쟁, 소비자 보호 : 우리의 현재와 미래

Abstract

Big Data and Privacy, Competition and Consumer Protection : Present and Future

Lee, Eun-woo

Big data refer to a technology to extract values from a large amount of typical or atypical data groups and analyze the results. Big data provide positive aspects such as efficiency, convenience and new utility creation but bring about various new problems such as infringement on privacy and equality, discrimination, economic inequality, threat on democracy, reduction of fair competition and deprivation of consumer rights.

There have been international efforts to solve these problems and the efforts of the ICCDP (International Conference of Data Protection and Privacy Commissioners and the Article 29 Working Party of the European Union are noticeable. They have stressed the importance in relation to profiling such as the maximum possible notification for transparency and trust, by-stage legal requirements at the operation stages, continued control of algorithm, human intervention in automatic determination and strengthened guarantee of the rights of a party to his/her personal data. They have maintained the necessity for additional legislation.

In the Republic of Korea, the Personal Data Protection Act guarantees the clarification of purposes, the principle of collection of minimum data and the rights to refer to, revise, and suspend processing of personal data. However, there is no regulation of automatic processing of personal data in relation to profiling. There is no duty prescribed to notice each element of profiling while the party's control over automatic processing of his/her personal data is maintained at an insignificant level.

On the other hand, in reality, the IT development, a widespread use of smartphones, permission of extensive data collection and sharing of financial institutions, collection and sharing of trade or credit card data by online and offline distributors, and accumulation of a large amount of public data have contributed to the current extensive generation, collection and use of personal

data. Additionally, a major corporate strategies is to collect, integrate and use the personal data collected extensively or other data generated in the business process.

A major future business strategy of SK Group, a representative communication and internet service provider includes advertisement, product sale and service provision through personal data of users. They collect various personal data through SK Telecom and SK Planet (data of smartphone use, map service, OK Cashbag service, and online shopping) and use them as a core business foundation. In their Personal Data Policy, they ambiguously state that ‘The company may collect the users’ data of use for tailor-made service or advertisement.’ There is no indication of the term or specificities of profiling.

The future business strategy of NAVER, one of the country’s representative internet portal services and its affiliates is advertisement, product sale and additional service trae through big data arising from personal data. As these companies take up more than 70% of the internet search, they collect personal data under the mobile environment and specify the strategy to secure them as a business platform. They collect the data under an ambiguous regulation in their Personal Data Policy that ‘The company may collect the data of the customer’s use of internet, mobile app and map service to provide tailor-made advertisements and personalized services.’ There is no clear indication of the period for data conservation. The profiling is not specified in terms of contents, either. Also, NAVER and SK Telecom collaborate in the big data area based on their respective data and develop joint businesses.

Korea has many large conglomerates and their dominance becomes stronger and the personal data platform of major companies is highly likely to infringe on privacy and consumer rights while damaging fair competition and intensifying the concentration of economic power. Preventing such problems require the assurance for more control of a party over personal data as to how the data extensively collected by large companies will be used in profiling. It is also necessary to whether the rights have been secured or the personal data protectio laws have been violated.

Under these circumstances, it is very urgent to clearly define the scope of the duty of notification in relation to profiling in the Personal Data Protection Act and revise the law toward a direction to guarantee the rights of an individual party to be involved in automatic processing. Recently, there is an opinion that the definition of personal data shall be reduced and only the data enabling identification of a person pertain to the data requiring advance agreement and

that other data shall be notified to a person in relation to processing and the person shall have the rights to refuse the processing, an opt-out method. This is a very dangerous position as it will fundamentally destroy the self-control of an individual party to his/her personal data especially in the country where the collection, identification and combination of personal data are very easy and widely conducted.

Keyword: Big Data, Profiling, Algorithm, Control over Profiling, Personal Data Profiling of Large Conglomerates, Tailor-made Advertisement and Personalized Services

빅데이터와 프라이버시, 공정경쟁, 소비자 보호 : 현재와 미래

이은우(법무법인 지향)

빅데이터의 명암

빅데이터

빅데이터

- 기존 데이터베이스 관리도구로 데이터를 수집, 저장, 관리, 분석할 수 있는 역량을 넘어서는 대량의 정형 또는 비정형 데이터 집합
- 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술.

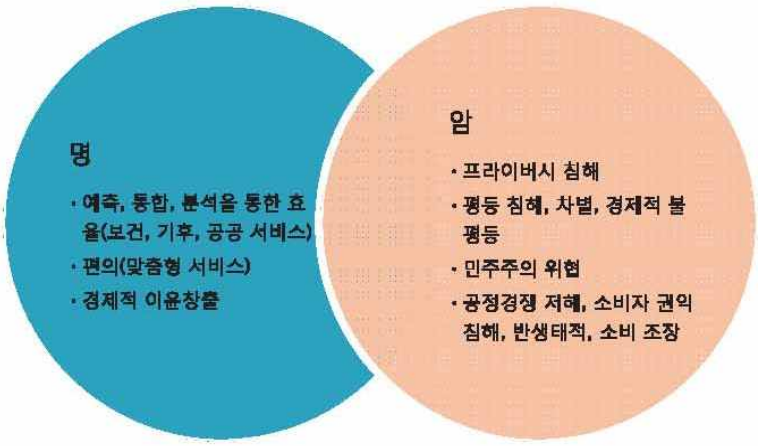
3V

- 규모(volume) – 대규모 분석. 양의 증가가 질적 차이를 만듬.
- 다양성(varelty) – 다양한 원천, 정형, 비정형적 데이터. 복합 분석. 데이터의 양을 획기적으로 늘림. 복합 분석으로 새로운 가치
- 속도(velocity) – 실시간 분석, 적시성.

각 단계별 다양한 이슈

- 수집 → 프로파일링(분석, 알고리즘) → 적용

빅데이터의 명암



빅데이터의 문제점

프라이버시의 침해

- 개인이나 집단에 대한 지나친 분석과 추적으로 평온한 삶 침해
- 꺼리는 사생활이 노출되거나 노출될 위험
- 사유의 자유 침해

평등침해 – 차별

- 분석, 프로파일링을 통한 범주, 낙인, 배제
  - 자동화 알고리즘의 차별 – 기존의 차별적 결과를 그대로 반영. 차별의 강화
- 정치, 경제, 사회, 문화적으로 차별
- 서비스 공급자의 차별적 공급(정치적 성향, 소득 수준 등)

민주주의 위협

- 공공성 약화
  - 누가 플랫폼을 설계하고, 운영하는가 – 공공에서 독점 사업자의 손으로
  - 공론의 상업화
  - 사회 관계망의 상업화
- 감시, 추적
- 표현의 자유 위협

빅데이터의 문제점

공정경쟁 저해

- 플랫폼
  - 정보의 이너서클(정보를 공유하는 자들과 배제되는 자들)
  - 네트워크 효과 강화(인프라, 정보집중)
- 폐쇄적 협력, 대기업 집단에 유리
- 불공정 경쟁

소비자 권익 침해

- 선택권 침해
- 정보불균등 – 마케팅의 희생자
- 불필요한 소비

반생태, 반환경

- 소비조장
- 반 생태적

빅데이터와 관련된 국제적 논의

빅데이터와 관련한 쟁점들

빅데이타 처리에 대한 원칙

- 기존의 원칙 vs 기존의 원칙 +
- 2013 EU WP 29 의견서
  - 목적 명확화, 최수 수집과 관련
  - 동의의 요부, 방법
  - 익명화
  - 빅데이터 처리 허용 여부의 판단
- 미국 FTC 접근
  - Reclaim your name

프로파일링에 대하여

- 과거 : 자동처리에 의한 의사결정에 초점
- 최근
  - 프로파일링에 대한 새로운 규율
  - 2012 ICCDP 선언, 2013 ICCDP 결정
  - 2013 EU 29 WP 의견서

빅데이터와 관련한 쟁점들

공정경쟁

- 플랫폼, 인프라 사업자와 지배적 지위 남용
  - 남용
    - 사업자들 사이에서
    - 소비자와의 관계에서
  - 영역
    - 포털
    - 통신사
    - 기기 제조사
- EU 구글에 대한 조사

빅데이터와 관련한 쟁점들

소비자 보호

- 더 많은 규제들 인정함.
- 공정한 표시
  - 표시에 대한 규제
- 소비자 단체
  - 특별한 역할 인정(공표, 소송, 비교 등)
  - 신속한 구제
- 약관 규제
  - 동의가 있어도 불공정성 판단

민주주의

- 표현의 자유
- 차별 금지

빅데이터와 관련된 국제적 논의

검색엔진, 쿠키, SNS, 스마트폰 앱

- EU Directive, EU 29 WP Op
- 캐나다, 미국 등

행태광고에 대하여

- 동의 여부
- 고지, 선택권
- 소비자 보호, 약자 보호, 미성년자 보호
- 미국, 유럽연합(EU WP 29 의견서), 한국

익명화, 익명처리에 대하여

- 과거 : 최소수집, 목적달성 폐기
- 최근 : 프로파일링과 관련하여 다시 제기
- 익명처리의 기준(영국 ICO)

ICCDP의 우루과이 선언(2012)

ICCDP(International Conference of Data Protection and Privacy Commissioners)

- 국제 개인정보보호 감독기구 회의
- 2012년 우루과이 회의에서 채택

배경

- 다양한 원천으로부터 수집한 정보를 바탕으로 프로파일링을 할 경우, 정보의 정확성, 최초 수집시의 목적과의 불일치 등으로 위험이 큼.
- 이와 관련한 개인정보 보호 원칙이 중요하며, 목적 제한의 원칙이 매우 중요함.

투명성과 신뢰 – 최대한 고지

- 고지할 내용 – 수집되는 방법, 프로파일의 사용 목적 등을 정보주체에게 알려야 함
- 더 잘 고지할수록 개인은 그의 데이터에 대해 더 잘 통제할 수 있다.

운용의 단계에서의 3단계 검토

- 먼저, 프로파일링을 이용할 필요가 있는지 여부에 대한 판단이 이루어져야 한다.
- 둘째, 어떤 가정과 어떤 데이터가 프로파일링의 기초를 형성할지를 결정해야 한다.
- 셋째, 실제로 프로파일이 어떤 방식으로 적용될지를 결정해야 한다.
- 각 단계별로 분리해서 판단하고, 별도 감독이 이루어지는 것이 바람직하다.

ICCDP의 우루과이 선언(2012)

알고리즘

- 지속적으로 프로파일과 기반을 이루는 알고리즘이 정당한지 여부를 확인해야 한다. 즉, 프로파일링의 결과가 유의미하며, 투입된 데이터와 합리적으로 연계되는지를 통제해야 한다는 것을 의미한다.

인간의 개입이 필요함

- 이는 특히 보다 효과적인 알고리즘으로 인해 프로파일링의 예측력이 향상되었기 때문이다.
- 완전 자동화로 인한 잘못된 결정으로 개인에게 부당한 영향이 있어서는 안된다.

프로파일의 생성과 적용의 분리

- 프로파일의 생성과 적용이 동일인에 의해 이루어지는 것은 바람직하지 않다. 프로파일을 생성하기 위한 정보와 실제의 적용 사이에 균형이 있어야 있어야 한다.

감독과 개인정보 주체의 권리보장

- 특히 프로파일링의 실제 적용 단계에서 개인이 프로파일과 결과 각각에 대하여 이의할 수 있는 권리가 보장되어야 한다.
- 강력하고 독립적인 개인정보 감독기구
- 프로파일링은 공공, 민간 분야 모두에 대한 감독권이 있는 강력하고 독립적인 감독 집행기구를 필요로 한다. 그 기관은 프로파일링 등에 대한 최신의 기술에 대해 필요한 모든 지식을 갖추고 있어야 한다.

정부에 대한 감독

- 정부는 민간분야에서 수집한 데이터가 포함된 다수의 대규모 데이터베이스에 접근할 수 있고, 스스로의 법적 근거를 만들 수 있기 때문에 프라이버시 감독기구가 감사, 빕플안 검토 등의 방법으로 정부의 법안을 검토하고 이의할 수 있어야 한다.

ICCDP의 바르샤바 결정(2013)

명확하게 확정

- 프로파일링을 시작하기 전에 미리 특정한 프로파일링 운용의 필요성과 실제 용도를 명확하게 확정하고, 적정한 보호조치가 마련되어야 한다.

제한, 최신성과 정확성

- Privacy by design의 원칙에 부합하도록 가정과 데이터의 양을 의도한 적법한 목적에 필요한 범위의 수준으로 제한. 데이터는 가능하다면 의도된 목적에 충분하도록 최신성과 정확성을 보장해야 한다.

지속적 확인

- 결과를 향상시키고 오류를 줄이기 위해서 프로파일과 알고리즘이 지속적으로 확인되어야 한다.

고지와 통제

- 가능한한 최대한의 범위에서 프로파일의 결합 방법, 프로파일이 사용되는 목적을 포함하여 프로파일링 운영에 대해 사회에 알려야 한다. 그리고 개인들이 가능하고, 적절한 최대한의 범위에서 개인정보에 대한 통제권을 유지할 수 있도록 보장하여야 한다.

접근, 개입

- 개인에게 중대한 법적 영향을 미치거나, 개인의 이익이나 지위에 영향을 주는 결정에 대해서는 그 개인에게 그의 접근권, 수정권과 인간의 개입권이 보장되어야 한다.

감독

- 모든 프로파일링 운영에 대해 적절한 감독이 이루어져야 한다

EU WP 29 수집과 이용의 제한에 대한 의견서

목적 제한(Purpose Limitation)

- 목적의 특정과 목적의 호환성

목적의 특정

- 목적은 반드시 :
- (i)특정 – 목적은 정보처리자에 의해 반드시 사전에 정의되어야 하며 정보주체가 어떤 처리가 가능하고, 어떤 처리는 불가능한 지를 구별할 수 있도록 알려져야 한다.
- (II) 명시적 – 목적은 정보주체가 알 수 있도록 하고, 합리적인 기대에 맞추어야 한다.
- (iii) 합법적 – 목적은 합법적이어야 한다.

호환가능한 이용

- 개인정보가 최초 수집된 것과 호환할 수 없는 용도로 처리되어서는 안된다.
- 모든 경우에 호환가능한 이용인지가 아래의 사항을 포함하여 개별적으로 평가되어야 한다.
  - 개인정보가 최초 수집될 때의 목적과 추가로 처리하고자 하는 목적의 관계
  - 개인정보가 최초 수집될 때의 맥락과 추가적 사용에 대하여 개인정보 주체가 합리적 기대를 했는지
  - 개인정보의 속성과 추가적 사용에 따른 개인정보 주체에 미치는 영향
  - 개인정보 처리자가 공정한 처리를 보장하고, 개인정보 주체에 미칠 부당한 영향을 막기 위해 취하는 안전조치

EU WP 29 프로파일링에 대한 의견서

프로파일링에 대한 분명한 정의 규정과 규율이 필요하다

- 프로파일링의 정의
  - "프로파일링"은 개인의 특성이나 개인의 어떤 측면, 특히 개인의 건강, 경제적 상태, 업무 처리, 개인의 취향, 관심, 행위의 신뢰성, 위치나 이동에 대한 분석이나 예측을 위한 개인정보의 자동화된 처리를 의미한다.

빅데이타 처리의 두 가지 경우를 구분

- 추세나 정보의 상호관계를 밝히기 위한 경우
  - 비밀유지, 데이터의 안전성, 기능적 분리를 보장하기 위해 필요한 기술적, 조직적 수단을 갖추어야 한다.
- 개인의 취향, 행동, 태도를 분석하거나 예측하기 위한 경우
- 거의 언제나 자유롭고, 특정되고, 충분히 인지되고, 모호하지 않은 사전 동의가 있어야 한다. 특히 직접 광고(Direct marketing), 행태 광고, 데이터 판매, 위치 기반 광고, 추적 기반 디지털 시장 조사(digital market research)의 경우
- 그렇지 않은 경우에는 추가적 사용은 호환가능한 것으로 볼 수 없다.

EU WP 29 프로파일링에 대한 의견서

프로파일링에 대한 규율 – 더 투명하게

- 정보주체에게 상세한 정보를 제공해야 한다
- 정보주체의 정보가 프로파일링의 목적으로 사용되고, 프로파일을 생성하게 될 것이라는 점을 인식해야 함,
- 어떤 목적으로 프로파일링이 이루어지는지 알아야 함,
- 자동화 절차의 내재된 판단기준을 이해해야 함.

정보주체의 강화된 통제권

- 명시적 동의
- 추가적으로
  - 프로파일에의 접근권(Right to access the profile)
  - 수정, 삭제권,(Right to modify or to delete the profile)
  - 프로파일에 의한 조치나 결정을 거부할 권리(Right to refuse any measure or decision based on the profile),
  - 이의를 할 권리(사람에 의한 개입 포함)

정보처리자의 책임성과 신뢰성이 더 필요

- 사전 영향 평가 필요
- 정보처리자에 의한 안전조치가 필요

EU WP 29 프로파일링에 대한 의견서

이익의 균형

- 추가적으로 이익 균형이 필요함. 반드시 사안별로 영향이 평가되어야 함. 그에 따라 적절한 조치가 취해져야 함.

위험의 평가

- 위험을 평가하기 위해서 호환 가능성, 안전조치의 평가가 필수적

공개

- 결정의 기준, 프로파일을 생성하게 한 데이터의 원천을 공개. 개인의 수정과 업데이트를 가능하도록 해야 함.

개인정보주체의 권리 강화

- 개인정보 주체의 권리 강화, 소비자와 정보처리자의 균형이 중요(개인정보 주체의 간편하고, 사용자 친화적 직접 접근권, 이익의 공유. 선택권 보장 등)

빅데이터와 우리 법률의 규율

현행 개인정보보호법

개인정보(개인정보보호법 제2조 제1호) 여부

- 생존하는 개인에 관한 정보로서, 특정한 개인을 알아볼 수 있는 정보(해당 정보만으로는 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우도 포함)

개인정보 보호 원칙(개인정보보호법 제3조)

- 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
- 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
- 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
- 개인정보의 처리 방법 및 형태 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
- 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
- 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
- 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
- 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

개인정보 주체의 권리(개인정보보호법 제4조)

- 개인정보의 처리에 관한 정보를 제공받을 권리
- 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
- 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
- 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
- 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

현행 개인정보보호법

수집시 고지사항(개인정보보호법 제15조 제2항)

- 개인정보의 수집, 이용 목적
- 수집하려는 개인정보의 항목
- 개인정보의 보유 및 이용기간
- 동의를 거부할 권리가 있다는 사실과 동의 거부의 불이익

제3자 제공시 고지사항(개인정보보호법 제17조 제2항)

- 개인정보를 제공받는 자
- 개인정보를 제공받는 자의 개인정보 이용 목적
- 제공하는 개인정보의 항목
- 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

개인정보의 파기

고유식별정보의 처리제한(개인정보보호법 제24조)

민감정보의 처리제한(개인정보보호법 제23조)

불확정적인 법률 개념과 그 해석

개인정보의 수집제한과 관련한 원칙

- 무엇이 목적에 필요한 최소한의 개인정보인가? 무엇이 정보통신서비스 제공을 위하여 필요한 최소한의 정보인가?
- 현행 개인정보보호법과 정통망법의 '목적에 필요한 최소한의 정보'의 범위를 어떻게 볼 것인지는 이익교량이 필요한 개념이다.
- 과도한 개인정보 수집인지 여부의 판단을 위해서는 각 개인정보의 유형, 개인정보의 집적 여부, 해당 목적과 정보주체의 이익 등 여러 요소를 고려해야 하는데, 개인정보의 유형별 해석지침이 필요하다.

개인정보보호법 제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
② 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조(개인정보의 수집 제한 등)
② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다.

동의를 받는 방법

- 명확하게 인지할 수 있도록 알린다는 것은 무엇을 의미하는가?
- 어느 정도까지 명확하게 알여야 하는지?
- 스마트폰이나 태블릿과 같은 기기의 경우는 어떻게 표시하야 하는지?

개인정보보호법 제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

우리나라 법률의 현황

개인정보 자동처리에 대한 규율이 없음

- 개인정보의 자동화된 처리와 관련한 정보주체의 권한이 충분히 보장되지 못함
- 자동처리에 대한 거부권이 보장되지 않음
- 자동처리에 대한 제한이 없음

프로파일링에 대한 정보주체의 권리가 미약함

- 프로파일링과 관련한 개인정보 주체의 통제권 미약.
- 정확한 고지가 되어 있지 못함.

두 가지 입장

옵트 아웃화론 - 개인정보 정의 규정 완화론

- 개인정보의 개념을 대폭 축소하고 대신 고지의무와 처리 거부권 신설하여 옵트 아웃화하자는 견해(2012, 최경진, 정준현, 지성우, 구태언)
- 현재 "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)로 정의.
- 괄호 부분을 삭제하자는 견해
- 단독으로 식별가능한 정보가 아닌 다른 정보와 결합하여 식별가능한 정보는 개인정보에서 제외해야 한다.
- 대신 프로파일링 처리 거부권 및 고지의무 신설. 이 경우 사실상 옵트 아웃화 됨.

두 가지 입장

개인정보 주체 권리보장 강화론

- 개인정보 주체의 프로파일링에 대한 거부권 규정이 없음
  - 개인정보 주체의 프로파일링에 대한 거부권 보장 필요
  - 자동화된 의사결정으로 인한 차별, 부당한 대우 가능성 높아짐.
- 개인정보 주체의 프로파일링에 대한 권한 미약
  - 개인정보 주체의 프로파일링 과정 전반에 대한 권한 보장 필요
  - 프로파일링에 대한 상세한 내용의 고지 의무 명확하게 할 필요
  - 개인정보 주체의 동의 및 선택권 보장
  - 데이터에 대한 이의권, 삭제, 정정, 처리 중단 요청권의 실효적 보장
- 개인정보 주체의 권리구제와 감독기능 강화
  - 개인정보 주체의 신속한 권리구제를 받을 권리 보장 및 감독기구의 권한 강화 필요

개인정보 주체 권리보장 필요

우리의 현실

- 이미 개인정보 및 데이터 집적이 매우 심각하며, 개인식별률이 매우 높은 현실
- 개인정보의 집중, 프로파일링은 경제력 집중을 강화하여 분배와 성장의 조화로운 발전에 반함.

프로파일링 관련 개인정보 주체 권리 보장 미약

- 입법적 미비를 보완할 필요.
- 우리 나라의 현실에 비추어 볼 때 개인정보 주체 권리보장 강화가 필요
- 입법과 고시, 가이드라인 제정 등 병행.
- 개인정보 주체의 권리구제 보장과 감독기구 권한 보장도 필요함. 이에 대한 법률 개정도 필요.

완화론

- 개인정보의 정의를 완화하여 옵트 아웃화 하는 것은 개인정보 자기결정권을 근본적으로 후퇴시키는 것으로 부당.
- 옵트아웃의 비율은 미약(5% 정도에 불과하다는 연구). 플랫폼 기업의 독점만 강화해 줌.

‘나’를 둘러싼 우리나라의 빅데이터 상황

‘나’에 대한 정보의 생성, 저장, 활용

범주별

- 공공, 민간
- 의, 식, 주, 교육, 사회, 경제, 문화, 정치

매체별

- PC / 스마트폰, 태블릿
- 신용카드, 금융거래
- 자동차(네비게이션)
- TV
- 기타(CCTV , 공공기록 등)

유형별

- 거래정보, 기호정보, 위치정보 등

‘나’에 대한 정보의 생성, 저장, 활용

인터넷 / 모바일

- 포털 : 네이버, 다음, 구글
- SNS : 트위터, 카카오톡, 페이스북, 라인, 틱톡, 밴드 등
- 모바일 앱

통신

- 이동통신(2013년 6월말 가입자수 5,410만명)
- 스마트 폰 가입자 수(2013년 6월말 가입자수 3,556만명, LTE 가입자 2200만명)

금융, 신용

- 금융지주회사 및 금융사 – 금융지주회사간 정보 공유
- 카드 거래 내역, 금융거래 내역, 신용관련 정보

유통

- 대형 유통사(온라인, 오프라인, TV)

TV

- 케이블, 위성, DMB, IPTV(752만)

우리나라의 특징

높은 본인식별

- 실명서비스 위주
  - 인터넷 실명제의 여파
  - 위헌 결정 이후에도 변하지 않는 정책

낮은 익명성

- 익명서비스 권리 확립되어 있지 못함

재식별 가능

- 핵심 식별자 역할을 하는 실명 식별된 식별자가 많음 – 주민등록번호, 휴대전화번호, 이메일, 트위터, 카카오톡
- 대부분 실명가입 강제하고, IP, 휴대폰 고유식별번호, MAC Address 등 식별가능한 정보 수집 보편화
- 익명화 조치에도 불구하고 재식별 가능. 익명화 조치를 했을 때 개인정보가 아닌 것으로 취급하기 어려움.

법제의 미비와 감독의 미비

우리나라의 특징

높은 IT 보급률로 데이터 방대함

- 초고속 인터넷 보급으로 인터넷 이용 활성화
- 높은 스마트폰 보급률로 방대한 데이터 집적 가능
- IPTV, 케이블 TV 보급

대규모 기업집단

- 대규모 기업집단 경제 집중 심화 및 기업집단 내외 제휴 활성화
- 대규모 기업집단의 개인정보 보유
- 신용카드, 유통, 통신, 통신, 스마트 기기 등

상호출자제한 대규모기업집단 지정현황					
년 도	2003	2006	2009	2012	2013
기업집단 수	49	59	48	63	62
소속회사 수	841	1,117	1,137	1,831	1,768
자산총액	652	873.5	1,310.60	1,997.60	2,108.10

순위	기업집단명	계열사수	자산총액
1	삼성	76	306.1
2	현대자동차	57	166.7
3	에스케이	81	140.6
4	엘지	61	102.4
5	롯데	77	87.5
6	포스코	52	81.1
7	현대중공업	26	56.5
8	지에스	79	55.2
9	한진	45	38.0
10	한화	49	35.9

우리나라의 특징

방대한 공공부문 보유정보

- 주민등록 정보, 부동산 등기 정보, 건강보험 관련 의료정보 등.

금융지주회사법과 금융정보 및 신용정보의 공유

- 금융지주회사등은 금융거래정보와 개인신용정보를 개인정보주체의 동의를 받지 않고도 그가 속하는 금융지주회사등에게 영업상 이용하게 할 목적으로 제공할 수 있다.
- 여기에는 금융거래 정보, 카드 사용내역 정보, 개인의 신용에 대한 정보 등이 모두 포함된다.
- 금융지주회사 사이에 이런 정보들이 공유됨.

금융지주회사 현황

우리	신한	KB	하나	농협	산은	SC	씨티	BS	DGB	한국투자	메리츠
자회사 등 구성	자회사12 손자회사 64	자회사 13개손자 회사18개	자회사10 손자회사 10	자회사10 손자회사 22	자회사7 손자회사 8	자회사5 손자회사 35	자회사5 손자회사 0	자회사3 손자회사 1	자회사6	자회사5 손자회사 0	자회사7 손자회사 14

사례를 통한 분석

SK 그룹과 고객정보

빅데이터 기반의 플랫폼 지향

스마트폰 발달로 모바일 인터넷 플랫폼의 형성

- 스마트폰/Tablet PC의 확산 및 네트워크 인프라의 대용량/고속화로 모바일 인터넷의 시대가 열릴 것
- 이에 따라 다양한 Content와 서비스를 중개하는 Application& Content Marketplace, N-screen 서비스 등 '플랫폼 사업'의 역할 및 가치가 확대될 것으로 전망.

LTE에서의 다양한 플랫폼 사업

- LTE로의 네트워크 진화
- 개인 방송 등 대용량 멀티미디어 스트리밍, 클라우드 기반 N-screen 서비스, 고화질 위치기반 서비스 등 다양한 플랫폼 사업의 기회가 확대.

고객, 빅데이타 → 광고, 커머스 → 플랫폼의 수익

- 초기에 가입자 및 Traffic 등 Power 기반의 Critical Mass 확보 후, 광고와 커머스 연계를 통해 수익을 실현하는 것이 플랫폼 사업의 속성
- 광고/커머스 시장의 최근 성장 추세는 플랫폼 사업자에게 새로운 기회로 작용할 것.
- 다양한 Data를 수집하고 활용하는 Big Data 기반의 플랫폼을 구축하고, Digital Contents와 커머스를 핵심 축으로 연계하여 고객 Benefit을 어우르는 미래형 통합 플랫폼의 중요성이 강화될 것으로 전망.

빅데이터 기반의 플랫폼 지향

Big Data 기반의 플랫폼 구축

- 국내 스마트폰 보급대수가 3,000만대를 넘어서는 등 다양한 Mobile Device의 확산
- 강력한 플랫폼을 가진 사업자가 ICT 시장의 주인공으로 부상
- 다양한 Data의 양적, 질적 팽창으로 인해 Big Data 기반의 플랫폼 구축을 통한 차별적 경쟁력 강화의 중요성이 부각됨

플랫폼

- 다양한 고객그룹들 간의 거래를 촉진하여 새로운 가치를 창출하는 중개 수단(Intermediary)
- 가입자와 이용자를 끊임없이 모여들게 하고 일정한 lock-in효과를 갖도록 하는 Ecosystem 형성이 중요
- 플랫폼은 기술적인 운영표준(IOS, Android OS), 가입자 기반 서비스 체계(Facebook, Twitter), 시장(Amazon, T store) 등 다양한 형태로 존재하며, 최근 '개방성'을 바탕으로 Global 확장이 가속화되면서 그 형태와 규모가 진화/확대되고 있음

플랫폼의 높은 성장 잠재력, 구글의 사례

- 플랫폼 사업은 다양한 인접서비스와의 연계성 및 Global시장으로의 확장 측면에서 아주 높은 성장 잠재력을 가지고 있음.
- Google의 사례
  - 수백만의 3rd Party를 광고 플랫폼인 애드센스로 끌어당김으로써 롱테일 광고라는 새로운 Ecosystem을 조성하였고, 모바일 시장에서도 안드로이드 OS를 기반으로 플랫폼 경쟁력을 확보하면서 높은 성장세를 보임.
  - 소비생활 전 영역에 걸쳐 구매행동 및 인식 패턴 정보를 분석할 수 있는 DB를 보유하고, 이를 활용하여 차별화된 서비스를 제공할 수 있는 Big Data 기반의 플랫폼 구축이 미래 핵심 경쟁 요소로 부각.

출처 : SKT 사업보고서(2013 반기)

빅데이터 기반의 플랫폼 지향

통신사인 SKT의 장점

- 단순히 기업 고객의 솔루션을 구축하거나 광고를 대행할 뿐 아니라 솔루션과 광고가 최종 소비자의 위치정보, 기호, 포인트·멤버십 등과 유기적으로 연계되어 기업 고객의 생산성·수익성 향상에 도움이 될 것 또한 요구되고 있음
- 통신사는 소비자에 관한 Big Data를 구축하고 있으며 지불, 고객 멤버십 등 다양한 고객 관련 서비스를 갖추고 있는 통신사들이 이와 같은 니즈에 효과적으로 대응할 수 있을 것임

SKT의 플랫폼 강화

- 플랫폼 영역에서는 자체적인 수익 창출도 중요하지만 모바일 광고, 개인의 소비패턴 에 관한 정보, 결제, 고객 포인트 제도, LBS 등과의 종합적 연계를 통해 수익으로 연결시키는 역량이 중요함.
- 또한 협력 기업들과의 Partnership, 개인화된 맞춤형 서비스 제공을 통해 플랫폼 자체의 경쟁력을 지속적으로 향상해 나갈 수 있어야 함

빅데이터 기반의 플랫폼 지향

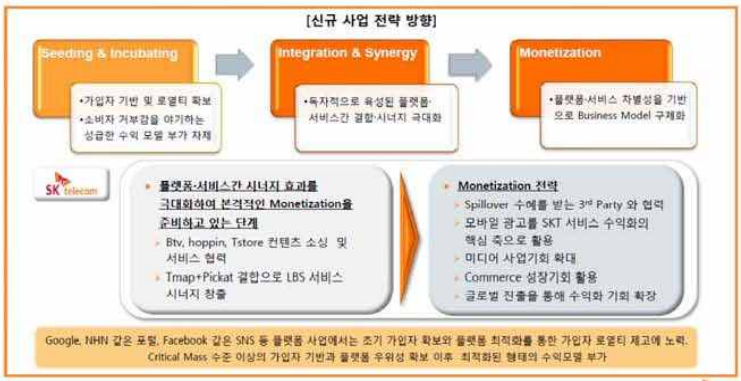
[통신사들의 플랫폼 사업 추진현황] "이제는 SK텔레콤 성장성을 볼 때다" 2013. 4.

플랫폼 서비스간 결합

신규 사업 Phase별 전략 방향

당사의 신규 성장사업 영역은 초기 육성 단계를 지나 역량과 서비스를 결집하여 실제 사업 성과를 창출하는 단계로 진행되고 있는 상황임. 당사는 사업 특성과 성장 Vision에 부합하는 구체적인 Monetization 전략을 구축·전개해 나가고 있음

[신규 사업 전략 방향]



3

"New Businesses –Ready to harvest" 2013. 9.

플랫폼 기반 정보 결합 활용

[참고] Connected Car 사업 현황

Connected Car 영역에서는 당사가 강점을 가지는 Tmap, 멀티미디어 등 서비스·컨텐츠 수익에 더해 모바일 회선을 탑재하는 등 신규 사업 영역의 수익화 기회를 확대하고 있음

[Smart nCare Service]

- 차량용 블랙박스, OBD(on-Board Diagnostic), 스마트폰을 연계하여 실시간 차량 운행 관리 서비스 제공
- 보험사 입장에서는 신속하고 신뢰성 있는 서비스 제공과 보상 비용 및 법률 비용 절감 등의 효과가 있음
- 동부화재가 마케팅 활동을 주도 하는 등 적극적 추진 중
- 향후 법인차량, 렌터카 등으로 고객 확대 예정

[Smart Car Service Platform]

- Tmap과 melon 서비스를 탑재한 서비스 플랫폼을 개발하여 르노삼성 전 차량에 적용('12년 9월 개시)
- 르노삼성 내비게이션 옵션 채택이 2.5~3배 증가
- 배터리 잔량 실시간 체크 및 주행거리 계산 등 전기차 전용 기능을 갖춘 서비스 플랫폼을 '13.10 르노삼성 전기차에 공급할 예정

[UBO Service]

- 기아차와 제휴하여 Smart Car Service 판매('12년 9월 개시)
- 이용료 9천원/월에 원격 시동/ 제어, 실시간 사고정보 연계된 긴급출동 서비스, 차량 진단 등 서비스 제공.
- 6천원/월 추가 시 음성통화 서비스, 1만원/월 추가 시 네이버 위치정보 서비스와 와이파이 존 서비스 제공

5

"New Businesses –Ready to harvest" 2013. 9.

모바일 광고가 수익의 축

Monetization 전략- 모바일 광고를 SKT 서비스 수익화의 핵심 축으로 활용

모바일 광고는 향후 신규 성장영역 Monetization의 핵심 축으로서의 역할을 담당할 전망. 당사는 그 동안 가입자 기반과 로열티 확보에 중점을 두고 육성해 온 미디어·서비스 수익화의 핵심 툴로서 모바일 광고를 적극 활용할 계획임

* Long-tail Economy: 대형 고객 중심에서 벗어나 방대한 규모의 중소규모 고객 기반으로 확장되어 부가가치를 높이는 사업 모델을 일컬음 (ex. Google 검색광고)
**설치율: 해당 앱 설치한 이용자 수/전체 모바일 인터넷 이용자 수

"New Businesses –Ready to harvest" 2013. 9.

고객 정보 활용한 수익 창출

Monetization 전략- Commerce 성장기회 활용

모바일 쇼핑은 eCommerce의 채널 확장 효과 외에도 새로운 서비스를 통해 Commerce 시장의 성장을 견인할 전망. 당사는 모바일 쇼핑 부문의 강점과 모바일 광고 등 다른 서비스와의 시너지를 통해 Commerce 사업의 수익화 기회를 확대해 나갈 계획임

"New Businesses –Ready to harvest" 2013. 9.

가입자 정보 - 수익의 원천

신규 성장영역 SK텔레콤의 강점

당사는 신규 사업 각 영역에서 ICT의 선순환적 생태계를 구축하고 수익화를 선도해 나갈 수 있는 역량과 사업기반을 보유하고 있음

"New Businesses –Ready to harvest" 2013. 9.

SK 빅데이터의 저수지

SK 빅데이터의 저수지

■ SK Planet continues to show strong growth led by 11st, T store and T map

Investor Presentation(2012. 11.)

모바일 광고와 연동

• SK플래닛 구조 조정 및 확장

SK M&C와의 합병

store

누구나 디지털 및 실물 콘텐츠를 사고 팔 수 있는 종합 콘텐츠 오픈마켓

T store는 2009년 9월 오픈 이후 현재 2,000만 가입자 중 월 평균 1,150만 명 이상이 무중의 하는 국내 최초 최대의 모바일 기반 종합 콘텐츠 마켓입니다. SK플래닛만의 콘텐츠와 플랫폼 역량을 결집시켜 앱, 게임, 영화, TV, 전자책, 쇼핑 쿠폰 등 다양한 카테고리에서 4만여 개가 넘는 풍성한 디지털 콘텐츠 및 실물 상품을 선보이고 있습니다. 누구나 앱을 등록하고 판매할 수 있는 열린 오픈마켓인 T store는 사전 검수를 통해 불법 비정상적 콘텐츠를 차단하고, 빈틈 없는 보안을 통해 콘텐츠에 대한 신뢰를 제공합니다. 또한 OTT(일회용 패스워드), 키스톡 등의 안전장치를 통해 결제 안정성은 물론, 다양한 결제수단 제공으로 결제 편의성을 높였습니다.
주소록 기반의 소셜 게임 API(Application Program Interface)를 배포하고, 글로벌 플랫폼과 입체의 채널을 확보 등 다양한 컨버전스로 모바일 서비스 시장을 선도하고 있는 T store는, 앱으로 여시아 시장을 중심으로 하여 사업을 확대하여 글로벌 마켓 플레이스로 진화할 것입니다.

모바일 마케팅의 종합솔루션 T ad와 함께하세요!

T ad가 확보하고 있는 다양한 매체에 정교한 Targeting으로 광고를 집행함으로써 광고주는 최대의 광고 효과를 얻을 수 있습
또한, SK플래닛만의 모바일광고 패키지 상품을 이용하여, 통합적인 모바일광고가 가능합니다.

• 모바일 사업 강화를 위해 SK M&C와의 합병 추진
- SK M&C는 OK캐쉬백 프로그램을 운영하였으며, 차량 네비게이션 및 기프트 쿠폰 등 일부 모바일 사업 운영

Premium Media Partners

T ad는 SK플래닛의 자산인 T store, T map을 비롯하여 전 국민의 SNS 싸이월드, 모바일 웹페이지 m.NATE, 글로벌 인기 게임 Angry Birds와 Rule the sky 등을 보유하고 있습니다.
또한, 보다 효과적인 모바일 마케팅 방법을 제공하고자 디매커진 등과 전략적 제휴를 맺어 다양한 리치미디어 상품을 개발하고 프리미엄 네트워크 영역을 넓혀가고 있습니다.

SKT Investor Presentation (2013. 09)

OK 캐쉬백과 제휴 및 프로파일링

- 3,600만명의 회원을 보유하고 있는 국내 최대의 통합 마일리지 서비스인 OK캐쉬백을 중심으로 다양한 프로그램을 제공하여 소비자가 기업의 제품과 서비스를 꾸준히 선택할 수 있도록 지원함.
- 최적의 마케팅 솔루션을 제공.
- 1999년 서비스를 시작한 대한민국 최대 통합 마일리지 서비스

마이샵과 중소 유통상인

마이샵과 중소 유통상인

마이샵과 중소 유통상인

발송된 쿠폰 사용내역을 고객별로 확인할 수 있어, 미사용 고객들을 대상으로
재발송 가능하며, 효율적으로 쿠폰관리 및 단골고객 관리를 할 수 있습니다.

서비스 사용료 : 월 5,000 원 (문자 쿠폰/SMS 250건 또는 이미지 쿠폰(MMS) 50건, 추가 사용 시 별도 충전 필요)

마이샵과 중소 유통상인

고객의 전화번호와 정보가 팝업창을 통해 표시되어
쉽게 고객정보를 확인할 수 있습니다.

고객이 매장으로 발신

고객정보 pop up

과거 주문이력이 자동으로 표시되기 때문에,
고객의 성향을 미리 파악하여
맞춤형 응대를 할 수 있습니다.

데이터의 프로파일링과 활용

○ 제공 DB

상권/업소/매출/이용자	잠재고객 : 유동/주거/주간	부동산 시세 및 개발 정보
업종 별 업소 현황 위치 및 밀집 지역	**업종 별 업소 현황** 위치 및 밀집 지역	**주요 시설 정보** 주요 시설 분포 현황 : 관공서/극장/병원 등 상권 주변 학교 분포 현황 교통시설의 위치/수
상권 내 총 시장 규모(총 매출) 상권 내 총 시장 규모의 증감 추이	**주거 인구** 주거 유형 별 주거 인구 증감 추이 주택의 형태 및 시세 정보 변화 추이 주거 인구의 성/연령/라이프스타일 변화 추이	**부동산 시세 및 거래 정보** 상권 내 권리금, 임대료 현황 및 변화 추이 상권 내 매물 거래 현황 및 변화 추이
상권 내 총 시장 규모(총 매출) 상권 내 총 시장 규모의 증감 추이	**유동 인구** 유동인구의 규모 시간대 별 유동인구 변화 추이 유동인구 유입 지역 변화 추이 유동인구의 /성/연령 /라이프스타일 변화 추이	**개발 정보** 분양 예정 상업/주거/사무용 시설, 시기 교통 관련 개발 정보 재개발/재건축 등 개발 정보
업종 별 업소 증감 추이 업종 별 업소 : 시구군/광역시도/전국비교	**주간상주인구** 주간상주인구 규모(현재는 기업체 정보)	
업종 별 매출 추이 시간대별 매출 비율 주중, 주말 매출 비율 성/연령 별 고객 매출 및 매출 점유율 단골고객 매출 점유율 고객당 1회 평균 소비 금액 : 객 단가 상권 내 일 평균 구매 고객 수 : 객 수	**기업체 및 종사자 현황** 외부 감사 기업	

SK planet 의 정보 활용과 프로파일링

T store

- 고품질의 Digital Contents 유통 서비스를 제공함으로써, T store 가입자 2,059만 확보('13년 6월 기준) 등 국내 No.1 Mobile 컨텐츠 오픈마켓을 구축
- '09년 9월에 론칭한 T store는 '13년 6월 기준 가입자 수 2,059만명, 누적 다운로드 13억건 등으로 국내 No.1 Application Store로서의 지위를 확고히 하고 있으며, 대상 단말 확대, 컨텐츠 강화, 개인오퍼링 강화 및 검색 고도화 등 Personalized Gateway & Mobile Play Ground로 진화하여 범글로벌서비스플랫폼으로 성장을 추진할 예정

T Store의 정보수집

- 이용내역 정보수집(선택 불가)
  - 서비스 이용 과정에서 다음과 같은 정보들이 자동으로 조회, 생성되어 수집될 수 있습니다.
    - 단말기 정보 및 서비스 접속 정보 (단말기 모델명, OS, 통신사, 단말기 식별정보(IMEI), MAC address, IP address, 방문일시)
    - T store 필수 프로그램 설치 정보 및 단말에 설치한 앱 정보 (명칭, 버전, 설치경로, 이용횟수, 이용시간)
    - 중복가입확인정보(DI), 암호화된 동일인 식별정보(CI)
    - 서비스 이용기록, 이용정지 기록, 이용해지 기록, 접속로그, 쿠키

SK planet 의 정보 활용과 프로파일링

T Store의 정보수집

- SK텔레콤 가입자의 경우 아래와 같은 정보들이 자동으로 생성되어 수집될 수 있습니다.
  - 휴대폰 명의정보, 가입요금제 (요금제 한도, PPS 여부), 번호변경/명의변경/기기변경/해지정보 등 휴대폰 관련 정보 변경 시 해당 정보, 서비스 관련 과금 청구/수납 정보
  - 유료 서비스 이용 과정에서 아래와 같은 결제 정보들이 수집될 수 있습니다.
    - 신용카드 결제 시: 신용카드 정보
    - OK캐쉬백 포인트 적립 및 사용 시: OK캐쉬백 카드번호
    - T 멤버십 결제 시: T 멤버십 카드번호 및 잔여포인트 정보
  - 그 외 더 나은 T store 서비스의 제공을 위해 해당 서비스 이용자에 한해서 아래와 같은 정보들이 수집될 수 있습니다.
    - 주소, 성별, Facebook ID

SK planet 의 정보 활용과 프로파일링

T Store의 정보수집

- 이용목적
  - SK 플래닛㈜ 상품/서비스(T map, T store, 11번가, hoppin, T cloud, Smart Wallet, T-ad, OK캐쉬백, 베네피아, 기프티콘, 틸리언패널, 스마트다이얼 등)에 대한 이용실적 정보 분석 및 개인맞춤형 배너 게재, 고객의 관심에 부합하는 서비스와 이벤트 기획 및 개인별 최적화된 서비스를 제공하기 위해 이용합니다.
- 위치기반 서비스 제공
  - SK플래닛㈜가 위치정보를 이용한 정보/광고 제공을 위해 위치정보를 보유하는 기간은 3개월간으로 하며, 이는 고객의 불만 응대등의 목적을 위하여 활용됩니다.
  - 그 외 신청인 및 법정대리인의 권리와 그 행사 방법, SK플래닛㈜의 주소/전화번호 등은 SK플래닛㈜의 위치기반 서비스 이용약관에 기재된 바에 따릅니다.
  - 본인은 위의 선택적 동의 내용을 충분히 숙지하였으며, 이에 동의합니다.(동의를 거부할 수 있으며 거부에 따른 불이익은 없습니다.)
- 정보보관 기간
  - 회원 탈퇴시까지

SK planet 의 정보 활용과 프로파일링

T store서비스 외 SK플래닛㈜의 정보/광고 수신 등의(선택동의)

- 본인은 본 서비스 외 SK플래닛㈜이 제공하는 서비스 관련 정보 및 광고 수신, 고객 만족도 조사에 동의하며, SK플래닛㈜는 본인이 본 동의를 철회할 때 까지 정보/광고를 지속적으로 제공합니다.
- 정보/광고 제공 내용
  - SK플래닛㈜의 상품, 서비스 또는 기타 타사, 제휴사가 제공하는 상품,서비스의 정보제공, 홍보,가입 권유 활동과 제반 프로모션 이벤트 활동, 선거/정치광고
  - 고객설문/시장조사 및 고객만족도 조사 등
  - 위치 정보를 활용한 상품/서비스 관련 정보/광고
  - 고객의 선호도, 라이프 스타일, 사회적 관계 등의 분석을 통한 개인 최적화된 정보/광고
  - 기타 타사, 제휴사의 list 및 상품/서비스의 상세 내용은 SK플래닛㈜의 정보/광고 제공서비스 홈페이지 www.skplanet.com에서 확인하실 수 있습니다.

SK planet 의 정보 활용과 프로파일링

T map 서비스

- 서비스 제공과정이나 업무 처리과정에서 다음과 같은 정보들이 생성되어 수집될 수 있습니다.
- 서비스 이용기록, 이용정지 기록, 이용해지 기록
- 접속로그, 쿠키, 접속 IP정보
- 회사는 다음과 같이 개인정보를 수집, 이용하며, 수집된 정보는 서비스 이용현황 통계/분석 활용에 이용될 수 있습니다.
- 수집항목: 이동전화번호, 통신사, 서비스 이용기록, 이용정지기록, 이용해지기록, 서비스 이용에 따른 위치정보 기록, 접속로그, 쿠키, 접속 IP정보, 단말기 Address (단말기의 고유 주소값), 법정 대리인 정보 (법정대리인과의 관계, 성명, 이동전화번호, E-mail 주소, 암호화된 동일인 식별정보(통신사, 이동전화번호)), 휴대폰 기종, 휴대폰 단말기 정보, T map필수 프로그램 설치 정보
- 수집/이용 목적: 이용자 확인, 찾아찾기, 최근길 정보 제공, 원활한 서비스 제공을 위한 기본 정보로써 이용, 서비스 관련 오류내용 확인을 위한 기초 데이터 및 불만 처리 용도로 활용, 서비스 이용현황 통계/분석 및 활용, 만 14세 미만 아동의 개인정보수집, 이용동의 확인, 원활한 서비스 제공을 위한 정보로써 수집, 서비스 제공과정이나 업무 처리과정에서 생성되는 정보, SK 플래닛㈜ 상품/서비스(T map, T store, 11번가, hoppin, T cloud, Smart Wallet, T-ad, OK캐쉬백, 베네피아, 기프티콘, 틸리언패널, 스마트다이얼 등)에 대한 이용실적 정보 분석 및 개인맞춤형 배너 게재
- 보유기간 – 고객님의 서비스 가입일로부터 고객님께 서비스를 제공하는 기간 동안

SK planet 의 정보 활용과 프로파일링

T map 서비스 – 국내 최고 수준 위치기반 서비스 플랫폼의 지위

- 지도, 주변정보, 실시간 교통정보 및 Navigation 서비스로 가입자 1,764만('13년 6월 기준)을 모집하였으며, 앞선 LBS 기술과 물류, 여행, 레저 등 타 산업과의 결합을 통하여 고객에게 새로운 편의와 가치를 제공
- 차량용 인포테인먼트 플랫폼을 적용하여 상용차 업체에 차량 장착 솔루션을 제공하는 등 LBS 플랫폼 기반을 확대해 나가고 있으며, 지역 정보와 광고를 연계하는 LBS 기반 Local Content 서비스를 제공
- 핵심자산인 Map, POI 등의 API Open을 통한 확장형 서비스 창출 유도, 대상 단말의 확대 및 지역 기반의 생활형 New LBS 서비스 개발 등으로 T map 플랫폼을 계속 발전시켜 나갈 계획.

정보 수집

- 쿠키 정보의 수집
- 쿠키(cookie)를 통해 수집한 회원의 아이디(ID)는 다음의 목적을 위해 사용될 수 있습니다.
  - 개인의 관심 분야에 따라 차별화된 정보 제공
  - 회원과 비회원의 접속 빈도 또는 머문 시간 등을 분석하여 이용자의 취향과 관심분야를 파악하여 마케팅에 활용
  - 관심 있게 둘러본 내용들에 대한 자취를 추적하여 다음 번 접속 때 개인 맞춤 서비스를 제공
  - 유료서비스 이용 시 이용기간 안내
  - 회원들의 습관을 분석하여 서비스 개편 등의 척도

SK Planet One ID

SK Planet One ID를 사용하는 곳

- T store(http://www.tstore.co.kr),
- T map(http://www.tmap.co.kr),
- T cloud(http://www.tcloud.co.kr),
- 11번가(http://www.11st.co.kr),
- OK캐쉬백(http://www.skcashbag.com),
- 상생혁신센터(https:/.oic.skplanet.com),
- Smart Touch Platform(http://www.sksmarttouch.com),
- Planet X 개발자센터 (http://developers.skplanetx.com)

One ID의 역할

- 개별적으로 수집된 정보의 통합 기준 역할
- 선택권 없음

SKT의 개인정보 수집 활용

SKT의 이동전화서비스 개인정보의 수집, 이용

- 개인정보의 수집 · 이용 목적
  - (1)서비스 제공 및 본인 식별 등 : 이동전화 서비스, 멤버십 서비스, **부가서비스, 제휴서비스, 개인맞춤서비스, 광고서비스 등** 제반 서비스(이하 '서비스') 제공 및 이와 관련된 본인확인 또는 인증, 통화품질 조사 등 서비스 품질 확인
  - (2)서비스 관련 정보 제공 등 : 상품 배송, 고지사항 전달, 본인의사 확인, 서비스 관련 상담 · 불만 처리, 서비스 이용관련 혜택 · 유의사항 · 편의사항 등 정보 제공, **신규 서비스나 이벤트 관련 정보 및 광고 전송**
  - (4)통계분석 : **개인을 식별할 수 없는 인구통계학적 분석자료** 또는 지역 · 시장 조사 자료(연령별, 성별, 지역별 통계분석, 시장 조사 등) 등 작성, 이용, 제공
  - (5)개인 맞춤서비스 제공 : **개인정보, 위치정보, 생성정보 및 이를 조합 · 분석한 정보를 이용한 요금제 등의 상품 및 서비스 개발** / 서비스 가입 신청 이용 중 문의 등 제반 고객 응대 시 고객 맞춤 상담 제공 / **개인 맞춤 상품 서비스 혜택 또는 개인 맞춤 광고 제안 및 제공**

SKT의 개인정보 수집 활용

SKT의 이동전화서비스 개인정보의 수집, 이용

- 수집하는 개인정보의 항목
- (1)식별정보 : 성명(법인명), 주민(법인등록번호), 여권번호, 외국인등록번호, 전화번호
- (2)연락처정보 : 주소, 전화번호, e-mail 주소
- (3)계좌정보 : 계좌(카드)번호, 예금주명 등
- (4)생성정보 : 발 • 수신번호(통화상대방번호 포함), 통화시각, 사용도수, 서비스이용기록, 접속로그, 쿠키, 접속 IP 정보, 결제기록, 이용정지기록, 멤버십 정보(멤버십 가입고객에 한함), 기타 요금 과금에 필요한 데이터 및 이를 조합하여 생성되는 정보(요약개인정보, 데이터마이닝 분석 및 고객세분화 정보, 선호도, 라이프스타일, 사회적 관계 추정 정보), Application 사용관련정보(사용 App.정보, 사용량 등) : 발•수신번호, 통화시각, 사용도수, 위치정보(기지국위치, GPS정보), 서비스 이용기록, 접속로그, 쿠키, 접속IP정보, 결제기록, 이용정지 기록 등 : 서비스 이용의 요금정산 및 위치기반 서비스, 개인맞춤 서비스 제공
- (5)기타 서비스 제공 관련 필요 정보 : 2.에 따른 개인위치정보, 단말기 정보(모델, IMEI번호, USIM번호, 단말기 S/W버전 정보 등), 직업, 국가유공자 증명 • 복지할인 증명 등 각종 증명, 부가서비스 • 번호이동 • 할부매매계약 내역, 이동전화 서비스 가입 및 해지일 • 이동전화 가입 기간 등

※ 위 정보는 가입 당시 정보뿐만 아니라 정보 수정으로 변경된 정보를 포함합니다.

- 개인정보의 보유 • 이용기간
- 서비스 계약 해지 시까지(단, 여러 서비스에 가입한 경우 일부 서비스에 대하여만 해지하는 경우는 제외)

SK planet 광고와 커머스 - 수익화의 핵심

T애드(T ad) Monetization의 핵심 영역으로 성장 기대

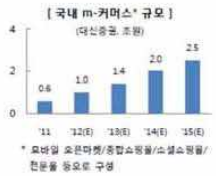
- 스마트폰이라는 작은 화면의 한계와 광고주들의 인식 부족 등으로 인해 모바일광고 시장은 아직 초기라고 핚 수 있으나, 웹에서 모바일로 급속히 전환되는 소비자의 사용 패턴을 고려 해 볼 때 모바일 광고 시장 전망은 매우 밝다고 할 수 있음
- 2012년 전세계 모바일 광고 시장 규모는 64억 달러, 2016년에는 236억 달러로 성장할 것으 로 보이며, 한국 모바일 광고 시장은 현재 미국, 일본, 영국에 이어 세계 4위 수준으로 2012 년 4.5억 달러, 2016년에는 7.6억 달러로 성장이 예상됨 (eMarketer, '12.7)
- 국내 모바일 오픈마켓의 선두주자위 SK플래닛의 모바일 11번가는 2012년 9월 말 현재 App. 다욲로드 수 1,100만건 달성, 2012년 3분기 누계 거래액은 전년도 실적 810억원의 두 배 이 상 초과하는 등 시장 리더십을 지속 강화해 가고 있음
- Gartner에 따르면 모바일 커머스 시장 규모는 2012년 753억 달러에서 2015년 2,341억 달러 로 성장할 것으로 전망되며, 대신증권은 국내 모바일 커머스 시장이 2012년 1조원에서 2015년 2.5조원으로 성장할 것으로 전망함
- ("지금이 SK텔레콤 가치 상승의 전환기" 2012. 11.)

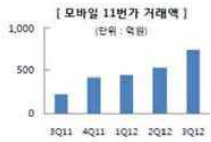
SK의 데이터 통합과 프로파일링

데이터 통합 – SK Planet 활용

- SK Planet One ID
- SK Planet의 개인정보 취급 수탁
- SK Planet의 플랫폼 사업

목표 – 광고와 커머스를 통한 수익의 창출





SK의 데이터 통합과 프로파일링

통합은 적정한가?

- One ID
  - 선택권이 보장되어야 함.
  - 최소 수집, 목적 적합성에 부합하기 어려움.
- SK Planet의 다양한 사업(11번가, OK 캐쉬백, T map, T store)
  - 다양한 사업이 개인정보의 통합을 위한 것임.
  - 개인정보가 분리되어야 함을 보장할 수 있는가? 보장하기 어렵다.
- 제휴사와의 정보 공유나 광고, 마케팅
  - 정보공유가 투명하지 않고, 광고나 마케팅 활용이 제한되어야 함.
- SK Planet의 개인정보 처리 업무 수탁
  - SK C&C, SKT 등의 개인정보 처리 수탁은 부적절함.

프로파일링은 적정한가?

- 투명성 부족
  - 구체적으로 어떻게 정보 수집하는지, 언제까지, 어떤 정보를, 어떻게 프로파일링하는지, 어떻게 사용하는지 등 불명확
- 개인정보 주체의 통제권 보장 안됨.

네이버

주식회사 네이버의 개요

- 1999년 6월 2일 인터넷 검색사이트 운영 등의 온라인 정보제공 사업을 영위할 목적으로 설립
- 엔에이치엔비즈니스플랫폼 분할. 한게임 분할
- K-IFRS기준 연결대상 종속회사는 37개사

2012년 매출액

- 연결기준 영업수익 2조 3,893억
- 검색광고(네이버 검색 결과에 노출되는 광고, 네이버 지식쇼핑 수수료) 1조 2,065억원
- 디스플레이 광고(네이버 페이지에 노출되는 디스플레이 광고, 네이버 지식쇼핑 부가광고) 3,466억원
- 온라인 게임 6,084억원
- 기타 2,277억원

검색서비스

- 회원 : 3,400만명, 월 순 3,180만명 방문
- 통합검색서비스
  - 지식IN, 블로그, 카페, 뉴스, 전문자료, 이미지 등
- 검색점유율(2013년 6월)
  - 네이버 74.0%,, 다음 19.8%, 구글 4.0%, 네이트 1.4%, Zum 0.8%

라인

- 세계 230여 개국에서 2억명이 함께 쓰는 글로벌 메신저(2013년 7월 기준)
- 1:1 채팅, 무료전화(m-VoIP, Mobile Voice over Internet Protocol), 그룹채팅, 이미지 및 영상공유 등을 모바일과 타블렛PC 및 PC에서 제공

밴드

- 2012년 8월 8일 출시한 이후 1,500만명(2013년 8월 기준)이 사용하는 지인기반 모바일 SNS서비스

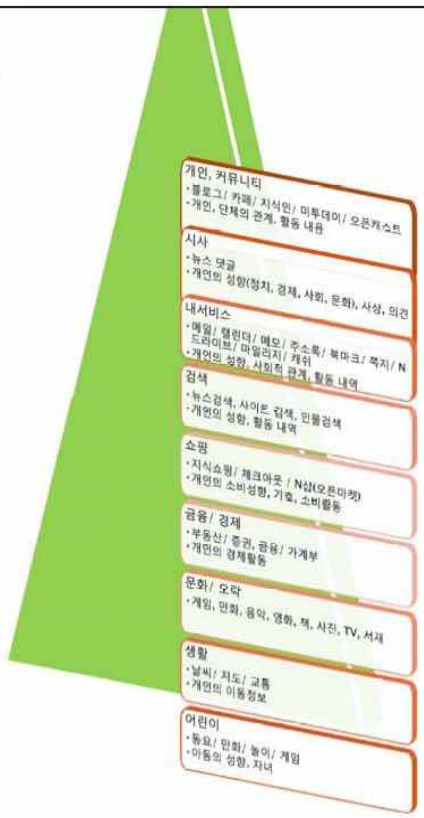
네이버 지식쇼핑

- 가격비교서비스

샵N 서비스

- 2012년 3월 오픈. 판매자가 자신의 상점을 직접 개설하고 상품정보를 등록한 뒤에 판매할 수 있는 온라인상품 플랫폼
- 블로그, 미투데이 등의 커뮤니티, 네이버 체크아웃을 통한 할인, 네이버 마일리지 적립 등의 서비스를 제공

네이버의 웹서비스와 수집하는 개인정보



네이버의 모바일 서비스

라인

라인 가입자 추이

사용자 1억명에 걸린 시간

네이버 앱

출처 : 네이버 다이어리

네이버의 모바일 앱

모바일 앱(영화, 여행)

<'타이탄의 분노' 영화정보> <미리보기 영상>

<네이버 원버스 모바일앱>

모바일 앱(지도, 교통)

2천만 다운로드 달성(출처 : 2013. 5. 네이버 블로그 기사)

네이버 개인정보취급방침

- **수집하는 개인정보의 항목 및 수집방법**
  - 서비스 이용과정이나 사업처리 과정에서 아래와 같은 정보들이 자동으로 생성되어 수집될 수 있습니다.
    - IP Address, 쿠키, 방문 일시, 서비스 이용 기록, 접속로그, 불량 이용 기록, 결제기록
- **컨텐츠 제공, 특정 맞춤 서비스 제공**
- **신규 서비스 개발 및 마케팅·광고에의 활용**
  - 신규 서비스 개발 및 맞춤 서비스 제공, 통계학적 특성에 따른 서비스 제공 및 광고 게재, 서비스의 유효성 확인, **이벤트 정보 및 참여기회 제공, 광고성 정보 제공**, 접속빈도 파악, 회원의 서비스이용에 대한 통계

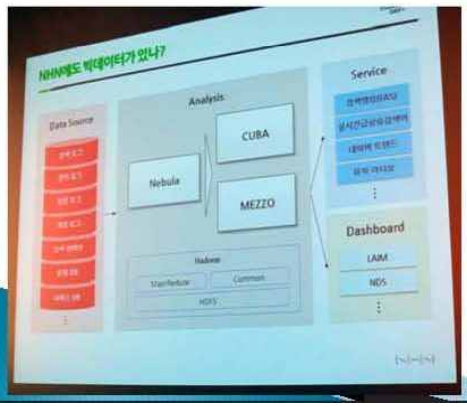
- **회사의 쿠키 사용 목적**
  - 이용자들이 방문한 네이버의 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부, 뉴스편집, 이용자 규모 등을 파악하여 이용자에게 광고를 포함한 최적화된 맞춤형 정보를 제공하기 위해 사용합니다.

- 회사는 개인화되고 맞춤화된 서비스를 제공하기 위해서 이용자의 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다.

네이버의 로그 데이터와 데이터 저장

- NHN의 로그 데이터 저장(2012. 12. NHN 커넥트 데이)
  - NHN은 2006년부터 모든 로그 데이터를 저장. 로그 데이터 중 필요한 정보만 빼내 저장하는 대신 이미지를 스캔하듯, 전체 로그를 스캔해 저장.
  - 시작은 검색 로그. 클릭 로그, 방문 로그, 게임 로그, 검색 컬렉션, 음원 DB, 서비스 DB로 확장.
  - 1일 발생하는 로그 데이터는 3TB

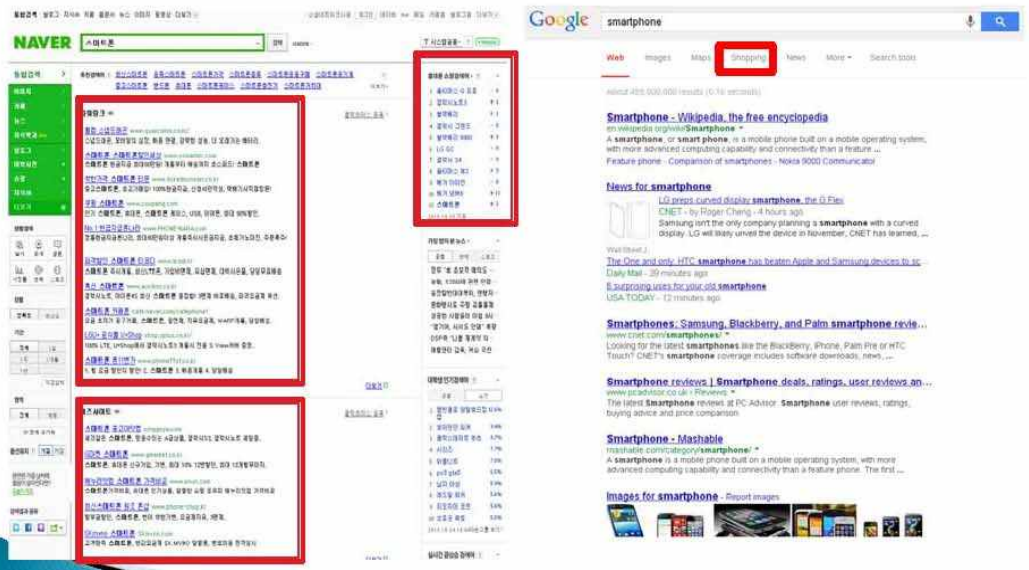
- 네이버 IDC 센터 '각'
  - 10년간 네이버 서비스로 만들어진 데이터는 약 180페타바이트(PB)
  - N드라이브에 하루 올라오는 데이터 400테라바이트(TB)



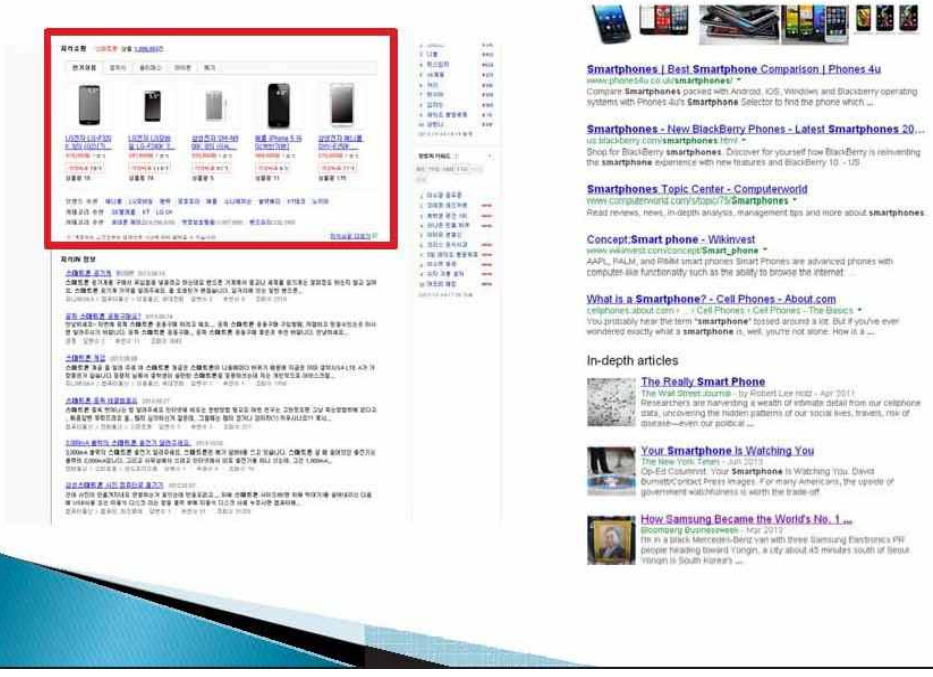
네이버 화면 구성의 변화

네이버 화면 구성의 변화

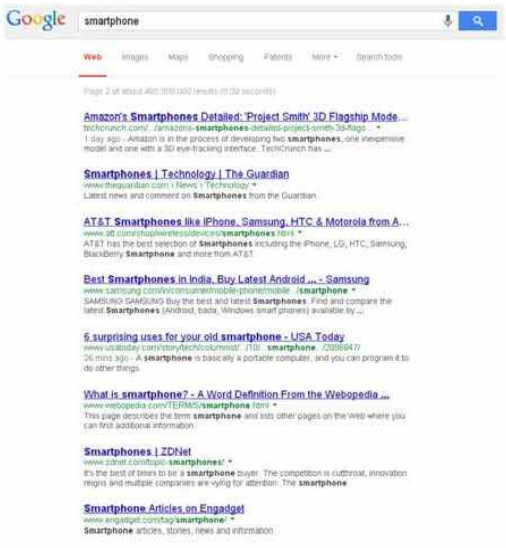
네이버와 구글의 검색결과 비교



네이버와 구글의 검색결과 비교



네이버와 구글의 검색결과 비교



네이버에 있는 데이터의 특징

수집되는 정보의 범위

- 데이터
  - 신문 보기, 댓글 달기, 궁금한 정보 검색, 전자우편 보내고 받기, 여행지 검색, 영화 검색, 음악 듣기, 상품 보기, 글쓰기, 사진 올리기, 카페 활동하기, 지도 보기, 부동산 정보 보기, 주식 정보 보기, 라인 대화하기 등.
- 로그 데이터
  - 사용자의 활동 내역을 추적할 수 있는 정보

특징

- 매우 민감한 정보
  - 민감 정보(정치적 견해, 신념, 사상, 건강, 인종, 종교 등)
- 매우 내밀한 정보
  - 사회적 활동에 관한 정보 포함
- 매우 다양한 정보
  - 영역 다양(거의 모든 영역)
  - 매일 방문하는 1,800만명의 거의 모든 생활, 1개월 3,280만명의 생활
  - 공개하는 정보와 익명성을 기대하는 정보의 혼재

네이버의 데이터 프로파일링의 문제

정보들의 결합시 개인에 대한 정보의 범위가 무한대로 확장됨

- 각 분야의 정보는 결합을 전제로 하지 않은 것이었음.
- 각 분야의 정보가 식별자를 매개로 결합될 경우 매우 민감하고 치명적인 정보가 됨.

부정확한 정보. 오해와 편견 야기할 정보 포함.

- 결합, 평가의 대상으로 될 것을 전제하는 정보가 아닌 것이 많음.
- 프로파일링의 대상이 되는 정보, 프로파일링의 결과, 목적을 모르는 경우 더 큰 문제.

익명성을 기대한 정보가 개인이 식별됨

- 익명정보가 개인식별이 될 매개가 많음(휴대전화, IP, 이메일 주소 등)

네이버는 어떻게 프로파일링하는가

현재의 개인정보 취급방침의 문제점

- 수집하는 정보의 범위 포괄적
  - 서비스 이용 내역(IP Address, 쿠키, 방문 일시, 서비스 이용 기록, 접속로그, 불량 이용 기록, 결제기록)을 수집한다고만 규정함
  - 구체적으로 어떤 정보를 어떻게 수집하는지 불명확함
- 정보수집의 목적과 활용범위 포괄적
  - "특정 맞춤 서비스 제공, 신규 서비스 개발 및 마케팅·광고에의 활용"
  - "신규 서비스 개발 및 맞춤 서비스 제공, 통계학적 특성에 따른 서비스 제공 및 광고 게재, 서비스의 유효성 확인, 이벤트 정보 및 참여기회 제공, 광고성 정보 제공, 접속빈도 파악, 회원의 서비스이용에 대한 통계"
  - "이용자들이 방문한 네이버의 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부, 뉴스편집, 이용자 규모 등을 파악하여 이용자에게 광고를 포함한 최적화된 맞춤형 정보를 제공하기 위해 사용"
  - "회사는 개인화되고 맞춤화된 서비스를 제공하기 위해서 이용자의 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용"
  - 맞춤 서비스, 최적화된 맞춤형 정보, 광고의 의미가 지나치게 포괄적
  - 익명성 보장도 안됨.

구체적인 프로파일링의 내용, 방식 등을 전혀 고지하지 않음.

- 현재는 거의 모든 정보를 수집하여 맞춤형 서비스, 맞춤형 광고를 제공하기 위해 사용할 수 있는 것으로 규정함.
- 어떤 정보를 어떻게 분석, 결합하여 어떻게 사용하는지를 밝히지 않음.

SKT와 네이버의 빅데이터 협력

2012. 11. 19. NHN-SKT, 미래 사업 발굴 위한 제휴 협약 체결

빅 데이터 사업 육성 협력

- 양사는 공동 프로젝트 그룹을 구성, 빅데이터 전문 인력과 기술을 상호 교류함으로써 각 산업분야에서 단편적으로 활용되던 데이터 분석/활용 경험과 기술을 융합하고, 기존 인프라 시스템을 강화하여 빅데이터 비즈니스 성공사례를 만들어 갈 계획이다

양사 서비스 결합을 통한 신규 서비스 개발 협력

- SK텔레콤의 스마트 네트워크 인프라와 NHN의 다년간 서비스 운영 노하우 결합을 통한 신규 서비스 개발 및 글로벌 진출 기회도 공동으로 모색한다.
- 양사가 보유한 데이터에 새로운 접근방법을 적용, 경영 혁신 방안을 도출함으로써 고객 니즈에 기반한 새로운 서비스 제공을 위해 협력하고, 맞춤형 서비스와 마케팅을 통한 효율성 증대도 이끌어낼 계획이다

소상공인 창업 지원 등 협력

- 다양한 사회 공헌 방안을 강구, 개인 및 기업고객, 공공분야 등 사회 전반으로 양사 제휴 협력의 효용을 확대해 나갈 예정이다.
- 가령 SK텔레콤의 상권분석 서비스와 네이버 지역정보 서비스를 결합, 소상공인의 창업 활동을 지원하는 방안 등이 검토될 예정이다

SKT와 네이버의 협력

SKT 전용 도들런처 무료 배포

- 런처 –
- 기본화면
  - 기본 화면에는 네이버의 각종 검색 서비스를 가장 앞에 내세웠다.
  - 기본 설치시 음성검색, 음악검색, QR코드, 와인라벨, 일본어 등 실생활에 유용한 서비스를 한데 모아뒀다.
- 'T서비스'
  - 폴더 하나에 스마트폰 이용자가 쓸 수 있는 SK텔레콤 서비스가 모두 모여있다.
  - 청구서나 모바일 IPTV, 모바일 클라우드 서비스, 네비게이션, 멤버십 등 여러 서비스를 'T서비스'란 이름으로 모아놨다.

제기되는 이슈

- 개인정보 보호
  - 상호 제공되는 개인정보는 SKT와 네이버에서 어떻게 활용되는가?
  - 추가적인 프로파일링의 가능성은?
- 공정경쟁 이슈
  - 모멜과 통신사의 상호 플랫폼 협력 강화로 공정한 경쟁이 보장되는가?

결론

결론

- 우리나라의 개인정보보호법제상 프로파일링에 대한 규정의 추가 및 권리보장 필요함.
- 각 기업들의 빅데이터 사업 추진은 투명하게 이루어져야 함.
- 각 기업의 개인정보 수집 및 공유, 활용 현실에 대한 실태 조사와 분석이 필요함.
- 우리나라의 정보 집적 현황을 고려할 때 개인정보 수집과 프로파일링은 공정경쟁의 관점에서도 보아야 함.
- 예컨대 SK 그룹, 네이버 등의 개인정보 수집을 통한 플랫폼화 시도는 개인정보의 보호, 공정경쟁, 소비자 보호 등 다양한 측면에서 타당성이나 문제점이 검토되어야 함.

국문초록

빅데이터와 프라이버시, 공정경쟁, 소비자 보호. 현재와 미래

이 은 우

빅데이터란 대량의 정형 또는 비정형 데이터 집합 또는 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술을 의미한다. 빅데이터는 효율성, 편의성, 새로운 효용의 창출과 같은 긍정적 측면도 있지만, 프라이버시 침해, 평등 침해와 차별 및 경제적 불평등, 민주주의 위협, 공정경쟁의 저해, 소비자 권익 침해 등 해결해야 할 여러 가지 새로운 문제를 야기하고 있다.

그 동안 이러한 문제를 해결하기 위하여 국제적인 노력이 있어 왔는데, ICCDP(International Conference of Data Protection and Privacy Commissioners, 국제개인정보보호감독기구 회의), 유럽연합의 Article 29 Working Party의 노력이 주목할 만하다. 이들은 프로파일링과 관련하여 투명성과 신뢰를 위하여 최대한 고지의 원칙, 운용의 단계에서의 단계별 적법성 확보, 알고리즘에 대한 지속적인 통제, 자동 결정에 대한 인간의 개입, 개인정보 주체의 권리 보장 강화 등이 중요하며, 이를 위한 추가적인 입법조치 등도 필요함을 강조해 왔다.

우리나라의 경우 개인정보보호법이 목적 명확화, 최소수집의 원칙, 개인정보 주체의 열람, 정정, 처리 중단의 요청권 등을 보장하고 있지만, 프로파일링과 관련해서는 개인정보 자동처리에 대한 규율이 없고, 프로파일링에 대한 각 요소별 고지의무도 규정되어 있지 않고, 자동처리에 대한 개인정보 주체의 통제권도 미약하게 보장하고 있다.

반면 우리나라의 현실을 보면, 개인에 대한 데이터의 생성, 수집, 활용이 정보통신 기술의 발달과 스마트폰 보급의 확산, 금융기관들의 광범위한 정보의 수집과 공유 허용, 온라인과 오프라인 유통업에서의 거래정보나 신용카드 정보의 집적과 공유, 막대한 공공정보의 축적 등의 요인으로 인해 방대한 수준으로 이루어지고 있다. 여기에 덧붙여 기업들은 대기업집단의 차원에서 그 동안 방대하게 수집해 온 개인정보나, 사업 과정에서 생성되는 개인정보를 수집, 통합하여 활용하는 것을 기업의 핵심 사업전략으로 삼고 있다.

대표적인 통신, 인터넷 관련 기업인 SK 그룹의 경우도 이용자의 개인정보를 기반으로 하는 빅데이터를 통한 광고와 상품 판매 및 부가적인 서비스 판매를 미래의

사업전략으로 삼고 있다. 이들은 에스케이텔레콤, 에스케이플래닛 등을 통하여 개인에 대한 다양한 정보(스마트폰 이용정보, 지도서비스 이용정보, OK 캐쉬백 서비스 이용정보, 온라인 쇼핑정보 등)를 수집하여, 이를 비즈니스의 핵심 기반으로 삼고자 한다. 이들은 이를 위해 개인정보취급방침에서 '이용자들의 이용내역에 관한 정보를 맞춤 서비스나 광고 서비스를 위하여 수집할 수 있다'고 모호하게 설명하고, 이를 수집하고 있는데, 보존기간도 분명하게 제시하지 않고, 구체적인 프로파일링의 내용도 밝히지 않고 있다.

대표적인 인터넷 포털 서비스 제공사인 주식회사 네이버와 그 계열회사들도 개인정보를 기반으로 하는 빅데이터를 통한 광고와 상품 판매 및 부가적인 서비스 판매를 미래의 사업전략으로 삼고 있다. 이들은 70%를 넘는 인터넷 검색점유율을 바탕으로, 모바일 환경의 개인정보를 수집하여 이를 비즈니스 플랫폼으로 확보하기 위한 전략을 구사하고 있다. 이들도 개인정보취급방침에서 '이용자들의 인터넷, 모바일 앱, 지도 서비스 등의 이용정보를 맞춤형 광고, 개인화된 서비스 제공을 위해 수집하여 이용할 수 있다'는 모호한 규정 아래 수집하고 있으며, 보존기간도 분명하게 제시하지 않고, 구체적인 프로파일링의 내용을 밝히지 않고 있다. 한편 주식회사 네이버와 에스케이텔레콤은 상호 협력도 추진하고 있는데, 각각의 데이터를 기반으로 빅데이터 사업에 협력하기로 하고, 공동사업을 추진하고 있기도 하다.

우리나라의 경우 대규모 대기업집단이 많고, 이들의 지배력이 강화되고 있는 상황에서 주요 기업군에 의한 개인정보의 플랫폼화는 프라이버시 침해의 위험, 소비자 권리의 침해 위험뿐만 아니라 공정경쟁을 저해하고 경제력 집중을 강화하는 결과를 야기할 위험이 크다. 이러한 위험을 막기 위해 대기업집단의 각 영역에서 막대하게 수집되는 개인정보가 어떻게 프로파일링되어 이용될지에 대해 개인정보 주체의 통제권이 보다 확실하게 보장되도록 해야 하고, 권리의 보장 여부, 개인정보보호법제의 위반 여부를 면밀하게 감독해야 할 필요가 있다.

이러한 상황에서 우리의 개인정보보호법에 프로파일링과 관련하여 고지의무의 범위를 명확하게 규정하고, 자동처리와 관련한 개인정보 주체의 개입권을 보장해 주는 방향으로의 법률 개정은 매우 시급한 과제이다. 최근 일각에서 개인정보의 정의를 축소하여, 그 자체로만 개인을 식별할 수 있는 정보만을 사전 동의가 필요한 개인정보로 보고, 그렇지 않은 개인에 관한 정보는 개인에게 처리에 대한 고지를 해주고, 처리 거부권을 주어 옵트아웃 방식을 도입하자는 주장이 제기되고 있는데, 이는 개인정보 주체의 자기통제권을 근본적으로 허무는 것이고, 우리나라와 같이 개인정보의 집적, 식별, 결합이 용이하며 광범하게 이루어진 상황에서는 매우 위험한 주장이다.

주제어 : 빅데이터, 프로파일링, 알고리즘, 프로파일링에 대한 통제권, 대기업집단의 개인정보 프로파일링, 맞춤형 광고 및 개인화된 서비스.

제5주제

빅데이터 환경과 개인정보의 보호방안

Abstract

Legal Methodology Concerning the Personal Information Protection while Considering Big Data Circumstance

Oh Gil Young

It was only a few years ago that we accepted the title, Digital Revolution. The internet access through personal computers and laptops, emails, and distribution of new contents such as digital images and MP3 sound sources brought about an enormous change in our lives. On the other hand, we are facing a new phase again. The earlier environment of digital revolution centering around devices and media gradually develops into a new form that works based on this network as the universal foundation.

Such an aspect reveals the start of a new ICT environment as well as new social issues. For example, the most recent example is the popularity of big data. It will be reasonable to state that the global internet industry concentrates on the new ICT environment where a large amount of data mass-produced from human digital activities are newly processed and commercialized. In line with the start of this big data environment, currently, there are large-scale discourses to revise the personal data protection policies. This means that the necessity to revise the current Personal Data Protection Act was maintained and the proactive criticism of major principles of the laws became available.

This paper started with a question as to the feasibility of these discussions. It is because there are perspectives other than incitement on new possibilities of the big data environment. It is also necessary to attentively observe the international movement where negative impacts of the big data environment or enormous backlashes often referred to as 'infringement on network privacy' or 'social hacking of personal data' become subject to public opinions. This paper will provide a review of discourses pertaining to revision of the laws related to personal data protection from a critical perspective based on the understanding.

This paper aims to provide a brief overview of the big data environment, sum up new legal issues arising from big data, and critically analyze new discourses trying to respond by overall revision of the laws related to personal data protection. Especially, from the perspective of data principals under the big data environment, the focus will be laid on the verification of specific feasibility in discussions pertaining to ‘re-organization of the concepts of personal data’ and ‘re-constitution of rights to consent’.

Keyword: Protection of Personal Data, Rights to Self-determination of Personal Data, Big Data, Opt-in, Opt-out

빅데이터 환경과 개인정보의 보호방안

— 정보주체의 관점에서 바라본 비판적 검토를 중심으로 —

오 길 영*

목 차

Ⅰ. 들어가며

지난 2011년부터 시행되고 있는 ‘개인정보 보호법(이하 개인정보보호법)’은, 긴 시간동안 비판받아온 바 있는 우리 개인정보 보호법제의 한계를 극복함과 동시에 많은 새로운 담론을 담아내고 있는 역작으로 평가받고 있다. 주로 공공부문에 대한 개인정보 보호에 머물러 있던 종래의 시각을 벗어던지고 민간부문에 대하여도 본격적인 규제를 상정하고 있다는 점, 현행의 디지털 환경을 제대로 반영해 내기 위해 다면적·다층적 고려가 있었음은 물론 많은 이해당사자의 담론들을 다각적으로 수렴하고 조율했다는 점은 부정할 수 없을 것이다. 이렇듯 오랜 진통을 견디어 탄생한 법률인 만큼 그 역할과 효과가 크리라 기대해 볼 수 있겠으나, 이러한 예측은 여지없이 깨어지고 있다. 법률이 시행되기도 이전부터 이미 비판이 시작된 바 있으며, 동법률의 시행으로부터 얼마지 않은 현 시점에는 이미 동법의 개정을 위한 본격적인 보고서들이 등장하고 있다.[1] 그 결정적인 동인은 바로 ‘ICT 토대의 전환’ 덕분이다. 이는 곧 또 다른 ICT 환경의 도래와 이에 의한 새로운 사회적 이슈가 발생하고 있음을 의미한다.

최근의 예를 들어 보자면, 소위 ‘빅데이터(Big Data)’ 열풍이 가장 대표적이다.

* 신경대학교 교수, 정보통신법

1) 최경진/황창근/신영수/이철남, 글로벌 환경 변화에 따른 미래 ICT 법정책 연구, 국가정보화전략위원회 연구용역 보고서(국가정보화전략위원회, 2012); 문재완/황성기/고학수/구태언/이인호/김기창/박광배/박경신/박상철/최경진/구본권/권영준/전응준/박병주, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013).

인류의 수많은 디지털 활동이 양산해내는 방대한 양의 데이터들을 새로이 가공하여 상품화할 수 있는 새로운 ICT 환경에 대하여, 지금 전세계 인터넷산업의 시선이 여기에 쏠려 있다고 해도 과언이 아니다. 물론 이렇듯 새로운 가능성에 대한 흥분의 시선[2]만이 있는 것은 아니다. '네트워크 프라이버시의 침해' 또는 '개인정보의 사회적 해킹' 등으로 표현되는 그 역기능에 대한 우려 또한 만만치 않은 시선으로 이를 노려보고 있기 때문이다.[3] 이렇듯 빅데이터로 통칭되는 새로운 패러다임의 등장은, 아직 제대로 걸음마조차 떼지 못한 신생 법률을 완전히 '올드패션'으로 취급하게끔 만들고 있다. 왜냐하면 빅데이터 논의와 궤를 같이 하는 개인정보 보호법제에 대한 수정담론의 대부분은 개인정보보호법의 오류와 미비를 지적하고 있기 때문이다.

그렇다면 개정을 하면 되지 않는가? 그러나 이 대답은 그리 쉽지만은 않다. 왜냐하면 개인정보보호법의 독특한 법적 지형을 고려해야 하기 때문이다. 즉 대상이 되는 개인정보는 비단 디지털 환경에서만 존재하는 것이 아니고, 동법이 뿌리내리고 있는 바탕이 오직 기술적인 기반만도 아니며, 나아가 동법이 구하고자 하는 법익이 비단 경제적인 것일 필요도 없기 때문이다. 또한 새로운 기술의 사회적 수용에 대한 고려가 선순환적 예측에 편향되어서는 안 된다는 점을 우리는 너무나 잘 알고 있기 때문이기도 하다. 따라서 지금의 시점에서 법학자는 필히 '검증과 형량'을 해보아야 한다. 먼저 기술의 보급과 그 완숙의 정도, 이를 통한 사회적 환경변화의 실재와 그 영향력, 법제도적 변화의 필요성과 그 정도 등에 대한 면밀한 검증이 선행되어야 하고, 이를 토대로 하여 구체적인 변화의 범위와 내용을 충돌하는 가치관들을 비교형량하면서 검토해 나아가야 한다. 이 글은 이러한 작업의 일환으로, 개인정보 보호법제에 대한 수정담론을 비판적 시각에서 검토하는 것을 주요한 내용으로 한다. 빅데이터 환경에서 발생하는 프라이버시 문제와 새로운 법적 이슈들을 요약해보고, 개인정보 보호법제의 총체적인 수정으로 대응하고자 하는 신생 담론들을 비판적 시각에서 분석하는 것이 이 글의 목적이다. 특히 빅데이터 환경하의 정보주체의 관점에서, '개인정보의 개념 재설정'과 '동의권의 재구성' 논의에 대한 구체적인 타당성을 검증하는 것에 초점을 맞추고자 한다.

---

2) "'빅데이터'는 당신의 미래를 내다본다", 아시아경제, 2013.5.25자; "빅데이터가 만드는 새로운 세상", 디지털타임스, 2013.5.24자; "'통찰&수익' 빅 데이터를 적극 검토해야 할 5가지 이유", CIO뉴스, 2013.5.23자; "대한민국 빅데이터, 어디로 가야할까", 디지털데일리, 2013.5.22자.

3) "'빅 데이터' 프라이버시 논의 시작할 때", ETNEWS, 2013. 5.24자; "속도붙은 빅데이터 부작용 최소화를", 디지털타임스, 2013.4.4자; "'빅데이터' 프라이버시 침해 우려, KSIDI 보고서-기업 빅데이터 분석과정 개인정보 무분별 활용-정부 규제 필요", 디지털타임스, 2013.2.12자; "'빅 데이터' 시대의 역기능을 막으려면?", 부산일보, 2012.11.21자.

Ⅱ. 거시적인 접근: 빅데이터와 프라이버시

1. 빅데이터 환경의 개관

1.1. 빅데이터의 개념

빅데이터 환경에 대한 각종의 자료들을 종합해보아도, 빅데이터는 말 그대로 '큰(Big) 자료(Data)'를 의미한다는 것 이상을 발견하기란 쉬운 일이 아니다. 그 정의에 관하여 구체적이거나 명확하게 합의된 바를 찾아내기 힘들기 때문이다. 빅데이터에 대한 주목은 아마도 시장조사기관인 가트너와 IDC[4]가 빅데이터를 2012년 주목해야할 세계적인 이슈로 꼽으면서부터 시작된 것 같다.[5] 대체적으로 빅데이터의 정의에 대해서는 "기존 데이터베이스 처리방식의 데이터 수집, 저장, 관리, 분석 역량을 넘어서는 데이터 셋"이라고 정의한 바 있는 맥킨지(McKinsey)의 개념설정[6]을 따르고 있는 것 같다.[7] 또한 "다양한 종류의 대규모 데이터로부터 저렴한 비용으로 가치를 추출하고, 데이터의 초고속 수집, 발굴, 분석을 지원하도록 고안된 차세대 기술 및 아키텍처"[8]라는 표현을 살펴볼 때, 데이터의 집합 자체를 넘어 플랫폼이나 분석기법 등 기술적 개념까지 포괄하고 있는 것[9]으로 판단해 볼 수 있다.

한편 빅데이터의 특징에 대해서는 대체로 일치하는 견해를 보이고 있다. 모두들 '크기(Volume), 속도(Velocity), 다양성(Variety)'을 의미하는 '3V'를 내세우고 있기 때문이다.[10] 여기서의 '크기'는 데이터 규모의 방대성을 말하는 것으로서, 빅데이터를 활용하려는 조직에서 그 수집·저장하여 관리·분석을 해야 할 데이터의 크기가 수십 테라바이트(Terra-byte, TB)[11]를 넘어 수 페타바이트(Peta-byte, PB)[12]에

---

4) Richard L. Villars/Carl W. Olofson/Matthew Eastwood, "Big Data: What It Is and Why You Should Care" (IDC, 2011), <http://sites.amd.com/us/Documents/IDC_AMD_Big_Data_Whitepaper.pdf> 검색일: 2013.10.5.

5) 이강용/남궁현/심재철/조기성/류원, "공공분야에서의 빅 데이터 활용을 위한 지식자산(Knowledge Base) 구축", 정보과학회지 제30권 제6호(한국정보과학회, 2012), 41쪽.

6) McKinsey Global Institute, "Big data: The next frontier for innovation competition and productivity" (McKinsey & Company, 2011), <http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx> 검색일: 2013.10.5, 1-3쪽.

7) 빅데이터의 정의에 관한 상세는 이강용/남궁현/심재철/조기성/류원, 앞의 글, 41-42쪽; 최경진/황창근/신영수/이철남, 앞의 보고서, 117쪽; 최경진/정준현/구태언/지성우/김도승/성준호, 빅데이터 환경에서 개인정보 보호 강화를 위한 법제도적 대책 방안 연구, 개인정보보호위원회 연구용역 보고서(개인정보 보호위원회, 2012), 5-8쪽 등.

8) Richard L. Villars/Carl W. Olofson/Matthew Eastwood, 앞의 글, 2-3쪽,

9) 최경진/황창근/신영수/이철남, 앞의 보고서, 117쪽.

10) 이강용/남궁현/심재철/조기성/류원, 앞의 글, 41-42쪽; 빅데이터의 정의에 관한 상세는 최경진/황창근/신영수/이철남, 앞의 보고서, 117-119쪽; 최경진/정준현/구태언/지성우/김도승/성준호, 앞의 보고서, 9-12쪽 등.

11) 테라바이트는 1,000 기가바이트(Giga-byte, GB), 즉 1조 바이트를 의미한다.

12) 페타바이트는 1,000,000 기가바이트(GB)를 의미하며, 이는 대략 17만 4천편의 DVD영화(약 6GB)를 담을 수 있는 용량을 말한다.

이를 만큼 그 양이 방대하다는 특징을 말한다. 다음으로 ‘속도’는 이렇듯 방대한 양의 데이터를 처리·분석하는 속도를 의미하는데, 데이터의 입·출력이 빠르게 증가하면서 이를 실시간으로 대응할 수 있는 빠른 처리와 분석의 능력을 말한다. 마지막 특징으로 이야기되는 ‘다양성’은, 분석해야 될 데이터의 형태가 종래의 정형데이터(Structured Data)[13]뿐만이 아니라 반정형(Semi-structured Data)[14]·비정형데이터(Unstructured Data)[15]까지 모두 포함하여 처리해야 됨을 의미한다.

이들을 함께 고려해 보면 결국 빅데이터는 단순히 크기가 방대한 것만을 의미하는 것이 아니라, 데이터의 생성과 소비가 매우 빨라 기존의 데이터 처리 방식으로는 관리·분석이 어려웠던 매우 다양한 형태의 데이터를 의미한다고 종합해 볼 수 있다.

1.2. 빅데이터 환경의 의미

빅데이터 환경은, 이러한 빅데이터를 가공하여 새로운 가치사슬을 구현해 내는 일련의 작업을 말한다. 이를 위해서는 ‘데이터의 생산자’라는 정보주체의 새로운 역할이 부여되고, 그 생산된 데이터를 수집·가공·활용·소비하는 새로운 ‘데이터 분석 시장’이 형성됨을 의미한다.

이러한 상상은 그리 어렵지 않게 해볼 수 있다. 현재 가장 뜨거운 주목을 받고 있는 모바일 기술이 이미 종래의 인터넷 환경에 더해져 융합되어버린 지는 오래고, 이제는 SNS 등의 모바일 서비스와 넘쳐나는 스마트 기기들 덕분에 그야말로 개인 데이터의 범람[16]을 경험하고 있기 때문이다. ‘이미지, 오디오, 비디오, 텍스트 등’ 각종의 비정형 데이터를 생산하게 되는 개인적 소통을 위한 서비스(예를 들어 SNS, 블로그, 유튜브 등)들은 이미 개인데이터의 폭증을 불러오고 있다. 이렇듯 우리의 일상 속에 이미 보편화되어 있는 다양한 스마트 서비스들은 빅데이터를 생성하는 원천이 되고, 따라서 그 서비스를 사용하는 정보주체는 ‘데이터의 생산자’의 지위인 것이지 누군가에 의해 만들어진 데이터를 단순히 사용만 하게 되는 ‘데이터의 소비자’에 불과한 것이 아니다. 즉 오늘날 정보주체의 모습은 소위 ‘PC 시대’의 컴퓨터 사용자와는 그 차원을 달리하는 것이다. 이러한 변화는 ICT 기술의 발전을 통해 빚어진 자연스러운 결과이며, 이미 우리의 일상 속에 공존하고 있는 현실이기도 하다.

한편 빅데이터의 가치는 이러한 현상적 의미를 넘어설 때 비로소 제대로 빛을 발하게 된다. 즉 1차로 생산된 개인데이터가 그 활용목적에 적합하게 재가공되어 사

13) 정해진 구조로 고정된 필드에 저장되는 데이터로서, 기존 관계형 데이터베이스(RDBMS)가 그 예가 될 수 있다: 이강용/남궁현/심재철/조기성/류원, 앞의 글, 43쪽.

14) 고정된 필드에 저장되지는 않지만 메타데이터나 스키마 등을 포함하는 데이터로 XML 또는 HTML 문서 등이 그 예가 될 수 있다: 이강용/남궁현/심재철/조기성/류원, 앞의 글, 43쪽.

15) 미리 정해진 구조가 없고 고정된 필드에 저장되지 않는 데이터로 일반 텍스트 문서, 이미지, 동영상, 음성 등을 예로 들 수 있다: 고정된 필드에 저장되지는 않지만 메타데이터나 스키마 등을 포함하는 데이터로 XML 또는 HTML 문서 등이 그 예가 될 수 있다: 이강용/남궁현/심재철/조기성/류원, 앞의 글, 43쪽.

16) 이유택, “빅데이터 시대의 개인 데이터 보호와 활용”, IT & Future Strategy 제8호(한국정보화진흥원 국가정보화기획단 정보화전략연구부, 2013), 1쪽.

회·경제적 가치를 창출하는 것이 가능해졌기 때문에, 지금의 빅데이터 열풍이 불고 있는 것이다. 현재의 ICT 기술은 정보주체 개인의 취향이나 사고, 행태는 물론 감정과 분위기, 습관이나 버릇에 관한 데이터까지 집적하고 분석해낼 수 있다고 한다. 어떻게 이러한 일들이 가능한 것일까? 예를 들면 GPS나 디지털 카메라 등의 센서들이 '개인이 어디를 방문하고 무엇을 쇼핑하는 것인지'를 구별해내는 소위 '라이프 로그(Life Log)' 정보를 자동으로 생성하고 있으며, SNS상의 메시지나 접속기록, 검색패턴은 물론 데이터 속성이 기록된 '그림자 데이터'까지 자동으로 수집되고 있기도 하다.[17] 또한 인터넷 플랫폼(인터넷 서비스 기업 또는 포탈 등)은 위치정보, 검색정보, 개인기호 등 다양한 문맥정보를 생성·관리하고 있으며, 이동통신회사나 디지털 기기의 제조회사들조차도 이제는 본격적으로 애플리케이션 서비스에 뛰어들면서 비정형 데이터가 생성되는 새로운 플랫폼으로 자리매김하고자 하고 있다.[18] 이러한 방식을 통해 수집된 방대한 데이터들은 집적·분석되어 가치창출을 위해 재가공된다. 즉 ① 국가의 공공질서 유지와 치안, 국가방위 등의 목적으로 활용되는 '공적인 가치', ② 소비행태, 소득수준, 생활양식이나 병력 등의 정보를 기업의 이윤창출에 활용하게 되는 '경제적·상업적 가치', ③ 취미나 특기, 성격이나 가치관, 경험 등이 공유를 위해 활용하게 되는 '사적인 가치' 등의 창출을 위한 데이터 분석시장이 형성되고, 이를 통해 빅데이터의 새로운 가치사슬이 형성됨은 물론 그 활용을 위한 플랫폼을 구성하게 된다.[19] 이것이 바로 빅데이터 환경의 면모이자, 빅데이터의 가치인 것이다.

2. 빅데이터 환경에서의 프라이버시

2.1. 개인데이터의 보호와 활용

빅데이터 환경 이전에도 개인정보는 이미 상품화되어 거래의 대상이긴 하였다. 그러나 빅데이터 환경에서는 개인정보의 성격이 '본격적'인 상품으로 전환된다는 점에서 양자는 차이를 보인다. 이는 결국 개인정보를 보호의 대상이자 개인정보자기결정권의 대상으로 보고 있던 우리 법제에 있어서는 큰 충격이 아닐 수 없다. 법적으로는 보호의 대상인 동시에, 사회적으로는 활용[20]의 대상이기도 하기 때문이다. 이러한 모순은 크게 3가지의 관점을 양산한 바 있다. ① 개인데이터의 활용에 주안점을 두고 열린 디지털 세계가 효율성과 안정성을 가져온다는 '유토피아적 관점', ② 정부와 기업이 디지털 프로파일 구축을 통해 개인을 통제할 우려가 있으므로 더욱 엄격한 보호정책과 규제가 필요하다는 '전체주의적 관점', ③ 프라이버시의 의미를 재정의하고 새로운 규제와 사업모델을 통해 개인데이터의 보호와 동

17) 이유택, 앞의 글, 1쪽.
18) 최경진/황창근/신영수/이철남, 앞의 보고서, 117-118쪽.
19) 이에 관한 상세는 이강용/남궁현/심재철/조기성/류원, 앞의 글, 42-45쪽; 최경진/황창근/신영수/이철남, 앞의 보고서, 117-118쪽; 이유택, 앞의 글, 3쪽 등.
20) 빅데이터의 다양한 활용에 대한 상세는 최경진/정준현/구태언/지성우/김도승/성준호, 앞의 보고서, 14-23쪽.

시에 그 활용도 모색해야 한다는 ‘절충적 관점’ 등[21]이 그것이다. 한마디로 말해 개인정보보호와 프라이버시 체제 전반에 걸친 대혼란의 시기인 것이다.

한편 빅데이터 환경은 기존의 프라이버시 정책이나 현행 개인정보 보호법제가 상정하고 있는 데이터 환경과도 부합하지 않는다. 왜냐하면 빅데이터는 단순히 데이터를 수집하거나 축적하는 수준에 머물지 않기 때문이다. 수집된 수많은 데이터들 속에서 가공의 목적에 적합한 데이터를 찾아내고 그 분석을 통해 상품성을 확보하는 일련의 과정을 거치게 되므로, 그 수집의 경로는 온·오프라인을 불문하고 그 형태는 정형·반정형·비정형을 구분치 않고 조합하게 되며 심지어 행태분석이나 패턴의 추출까지 진행하게 된다. 즉 다면적·다층적 분석을 통해 특정인에 대해 종합적이고 세밀한 결과를 도출하게 된다는 것이다. 따라서 만약 이를 통해 누군가에게 프라이버시 침해가 발생한다면, 그 침해의 정도는 종래와는 비교할 수 없는, 말 그대로의 ‘심대한 침탈’이 될 가능성이 농후하다. 다시 말해, 빅데이터 환경에서의 프라이버시 침해는 특정인의 생활과 가치관 그리고 그의 기억과 미래의 꿈들을 송두리째 무너뜨리는, 가히 치명적인 부작용을 가지고 오게 된다는 것이다.

2.2. 개인정보 보호법제의 수정담론

빅데이터 환경에서 발생하는 개인정보 보호와 프라이버시 체제 전반의 모순에 관하여, 우리나라 학계에서의 논의는 주로 ‘유토피아적 관점’에 치우쳐져 있는 것으로 판단된다. 대부분의 목소리가 현행 개인정보보호법의 한계를 주목하고 있기 때문이다. 즉 ① 개인정보의 정의나 기준 및 절차와 관련하여 디지털 시대의 태동기적 시각을 바탕으로 하고 있다는 점,[22] 그리고 ② 규제일변도로 치우쳐있던 과거 개인정보 보호정책이나 프라이버시 가치관이 현재 개방형 네트워크 문화에 적절하지 못하다는 점,[23] 나아가 ③ SNS, 클라우드 서비스나 행태기반 서비스 등 무서운

---

21) 이유택, 앞의 글, 4쪽.

22) 구태언, “현행 개인정보보호 법제상 ‘개인정보’ 정의의 문제점”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 이인호, “개인정보처리(수집이용제공)의 법적 기준에 대한 타당성 분석”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 김기창, “개인정보 주체의 ‘동의’: 동의의 허구성과 해결방안”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 박경신, “‘개인정보’의 정의와 위치정보보호법의 개선 방안”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 권영준, “개인정보 손해배상소송에 있어서 과실 및 손해 판단기준”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 전응준, “개인정보침해행위에 대한 형사처벌의 적절성”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 박병주, “개인정보보호법이 의학 및 보건학 연구에 미치는 영향”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013).

23) 문제완, “프라이버시 보호: 신화에서 규범으로”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 황성기, “개인정보 보호와 다른 헌법적 가치의 조화”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 고학수, “개인정보보호의 법, 경제 및 이노베이션”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 최경진, “개인정보 주체의 권리에 대한 조화로운 접근”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 구본권, “잊혀질 권리와 알 권리: 저널리즘적 관점에서”, 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013).

속도로 보급되고 있는 ICT 신기술의 새로운 국면에 무력하다는 점[24] 등이 주요한 내용이다. 물론 이를 두고 '유토피아적 관점'이 아니라 '절충적 관점'이라고 해석해 볼 수도 있을 것이다. 그러나 이에 대해 필자가 가지는 고민은, 점차 다수의 글들을 접하게 되면서 양자의 차이를 알기 힘들었다는 점이다. 또한 더욱 엄격한 보호정책과 규제가 필요하다는 '전체주의적 관점'에서 집필된 글[25]을 쉬이 찾기가 힘들었다는 점도 문제다.

이러한 국내의 상황과는 대조적으로 미국학계에서는, 이러한 우려의 관점에서 진행되는 논의들을 어렵지 않게 찾을수 있다. 빅데이터가 야기하는 심대한 프라이버시 침해가능성에 대한 날카로운 지적은 물론, 새로운 규제의 시작점과 구체적인 쟁점의 제시, 심지어 규제와 정책의 관점에서 빅데이터 자체의 모순도 지적하고 있다.[26] 유럽의 움직임 또한 마찬가지이다. EU는 지난 2012년 1월에 즈음하여, 종래의 '유럽위원회 데이터 보호지침(1995)'[27]을 계승·강화한 'EU 데이터 보호규정안(2012)'[28]을 발표한 바 있다. 동 규정안은 기존의 지침(Derective)에서 규정(Regulation)으로 격상되어 EU 전역에서 통일된 법령으로 기능하게 되는데, ① 정보주체가 자신과 관련된 개인데이터의 처리를 동의하기 이전에, 이에 대한 충분한 설명을 받을 권리를 규정하고, ② 정보주체는 자신의 데이터를 회수하여 다른 서비스로 이동시킬 수 있는 등 데이터의 이동성(Data Portability)을 보장하며, ③ 사망 후 자신에게 불리한 프로파일링의 대상이 되지 않을 권리는 물론 자신과 관련된 데이터의 삭제를 요구할 수 있는 잊혀질 권리(Right to be forgotten)를 규정하는 등 프라이버시 보호체제의 대대적 강화를 주요한 내용으로 하고 있다.[29]

---

24) 김기창, "클라우드 서비스와 개인정보보호", 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 박광배, "개인정보 국외이전의 실무적 문제와 개선방향", 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013); 박성철, "행태기반서비스(위치기반서비스 포함) 관련 법령 정비 방안", 개인정보보호법제 개선을 위한 정책연구보고서(프라이버시 정책연구 포럼, 2013).

25) 이에 해당하는 글로 필자가 찾아낸 국내논문으로는 이창범, "개인정보보호법제 관점에서 본 빅데터의 활용과 보호방안", 단국법학 제37권 제1호(단국대학교 법학연구소, 2013)가 유일하다.

26) Neil M. Richard/Jonathan H. King, "Three Paradoxes of Big Data", Stanford Law Review Online(2013), <http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_41_RichardsKing.pdf>, 검색일: 2013.10.5; Omer Tene/Jules Polonetsky, "Privacy in the Age of Big Data: A Time for Big Decisions", Stanford Law Review Online(2012), <http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf>, 검색일: 2013.10.5; Cynthia Dwork/Deirdre K.Mulligan, "It's not Privacy, and It's not Fair", Stanford Law Review Online(2013), <http://www.stanfordlawreview.org/sites/default/files/online/topics/DworkMullliganSLR.pdf>, 검색일: 2013.10.5; Joseph W. Jerome, "Buying and Selling Privacy: Big Data's Different Burdens and Benefits", Stanford Law Review Online(2013), <http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_47_Jerome.pdf>, 검색일: 2013.10.5 등.

27) Directive of the European Parliament of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC.

28) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012.1.25, <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>, 검색일: 2013.10.5: 동 규정안은 유럽의회를 통과할 경우 2년간의 유예기간을 거쳐 2014년부터 발효될 예정이다.

29) 지면관계상 상술할 여력이 없으나, 미국 오바마 정부도 지난 2012년 2월 '소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)'을 통해 개인데이터의 프라이버시 보호를 위한 전략을 제시한 바 있

III. 미시적인 분석: 수정담론의 비판

1. 개인정보의 개념 수정론

수정담론에서 가장 먼저 대두되는 쟁점은 현행법 체제의 개인정보 개념을 수정하는 것이다. 개인정보보호법은 제2조 제1호의 정의규정에서 “ 개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다” 라고 규정하고 있다. 이 정의에 의하면 동법의 보호대상이 되는 개인정보는 ‘살아있는 개인(생존성)’ 이라는 요소와 ‘정보로부터 해당 개인을 알 수 있거나(식별성)’ ‘다른 정보와 결합하여 쉽게 알 수 있을 것(결합성)’ 이라는 요건을 부과하고 있는 셈이 된다. 이러한 정의방식은 기타 관련법제에 있어서도 크게 다르지 않다. 즉 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률(동법 제2조, 이하 정보통신망법)’, ‘위치정보의 보호 및 이용 등에 관한 법률(동법 제2조, 이하 위치정보보호법)’, ‘전자서명법(동법 제2조)’, ‘국민의 형사재판 참여에 관한 규칙(동규칙 제44조)’, ‘금융실명거래 및 비밀보장에 관한 법률 시행령(동시행령 제6조)’ 등에서도 비슷한 형태로 규정하고 있다.[30]

1.1. 수정담론의 검토

수정담론은 ‘개인정보’ 를 곧바로 ‘프라이버시’ 로 취급하는 논리가 오류라는 바탕위에서 논의를 진행하고 있다. 즉 개인정보는 다양한 사회적 가치를 내포하는 ‘사회적 자본의 핵심 요소’ 의 성격도 가지고 있으므로 현행 개인정보 보호법이 ‘개인정보의 적정한 이용과 보호’ 가 아니라 오로지 개인정보의 보호 쪽으로만 치우쳐져 있는 것은 바람직하지 않다는 논리이다. 이러한 논리는 개인정보의 사회적 활용 필요성을 도외시하고 정보주체의 보호만을 제1의 가치로 내세우고 있는 현행 입법태도가 바람직하지 않으므로, 개정을 통하여 ‘개인정보의 적정한 이용’ 이 가능하도록 함은 물론 나아가 그 적정한 이용을 보장하기 위한 ‘공정이용’ 에 관한 새로운 조항까지도 마련해야한다고 주장한다.[31] 이러한 논리전개의 기저에는 우리 입법의 프라이버시 정책이 과거 권위주의 정부시절에 자행되었던 프라이버시 침해를 경험하고 얻은 일종의 ‘트라우마’ 의 산물이라는 시각이 깔려있다.[32] 그렇다.

다: White House, Consumer Data Privacy in a Networked World(2012), <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>, 검색일: 2013.10.5.

30) 다만 ‘신용정보의 이용 및 보호에 관한 법률’ 에서는 구체적이고 다양한 식별요소를 도입하여 그 범위를 제한하고 있어 이와는 상이하다(동법 제2조 및 동법 시행령 제2조).

31) 구태언, “개인정보보호의 새로운 패러다임”, 보안뉴스 기고문(2013), 1-2쪽.

32) 구태언, 앞의 기고문, 2쪽.

처참하기 그지없었던 우리네 프라이버시 관련사를 곰곰이 떠올려보면, 어쩌면 이러한 시각이 맞을지도 모르겠다. 그렇다면 이 지점에서 우리는, 이러한 현행 입법태도를 구성해낸 종래의 경험과 담론들에 대해 면밀하고도 비판적인 검증을 시행해 보아야만 한다. 지금까지 프라이버시 침해의 현상을 수집하고 분석한 많은 자료[33]들이 진정 트라우마로 인한 것들인지 말이다.

한편 이러한 수정담론의 입장은 현행의 개인정보 개념설정에 문제가 있다는 지적으로 이어진다. 즉 "살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)" 라고 규정하고 있는 현행 개인정보 보호법의 개념설정이 너무 광범위하여 큰 문제라는 주장이다. 즉 괄호 앞쪽의 정보(이하 전자)는 몰라도 괄호속의 정보(이하 후자)까지 동시에 규정하게 되면서 그 범주가 대단히 넓다는 것인데, 이 덕분에 기업의 영업활동이 극도로 위축되고 형벌을 지나치게 확장시키는 부작용이 발생하고 있다고 한다.[34] 이러한 논지는 결국 전자와 후자를 구별하여 차별적으로 취급하자는 주장으로 이어진다. 필자에 따라서 '개인식별정보와 사람관련정보'[35]로 설정하기도 하고 '개인정보와 개인에 관한 정보'[36]로 표현하기도 하나, 어찌되었건 양자를 구분하여 다르게 취급하자는 점에서는 대동소이하다. 이러한 논지는 대단히 실용적인 취지에서 시작되지 않았나 생각해 본다. 즉 전자가 제거된 후자만을 취급할 경우 사실상 익명화되어 개인정보성이 상실되므로,[37] 현재의 빅데이터 시대에 있어 가장 핵심적이고 주요한 경제적 자원으로 활용가능하다는 것이 그 이유가 될 것이다. 그러나 이러한 시도를 프라이버시 보호의 차원에 바라보면, 본격적인 '개인정보의 상품화'를 전제로 하고 있다는 점에서 심대한 우려가 발생함을 부정할 수 없다. 결국 개인정보의 개념의 재설정은 단순히 그 분류나 범위를 재획정하는 문제가 아닌 것이다. '개인정보의 상품화' 또는 '프라이버시의 상업화'를 어느 수준에서 수용할 것인가 하는 대단히 복잡하고도 민감한 법정책적 논제인 것이다.

1.2. 구체적인 분석

1.2.1. 식별성의 문제

개인정보의 개념설정이 광범위하다는 논지는 결국 '식별의 가부'를 요건으로 하고 있기 때문에 발생하는 문제이다. 즉 우리 개인정보법제가 취하고 있는 개인정보의 개념은 ① 원칙적으로는 개인식별정보(Personally Identifiable Information, PII)

33) 대표적인 자료로는 국회의원 진선미(민주통합당), 행정부문 개인정보 보호의 현황과 과제, 2012년 국정감사 정책자료집(2012); 진보네트워크센터, 개인정보 수집·유통 실태조사, 국가인권위원회 연구용역 보고서(2009) 등.
34) 구태언, 앞의 글(각주 22), 38-39쪽.
35) 구태언, 앞의 글(각주 22), 43-44쪽.
36) 황성기, 앞의 글, 19쪽.
37) 구태언, 앞의 글(각주 22), 43-44쪽.

를 상정하고 있으면서, 동시에 ② ‘해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함’하므로 ‘비식별정보(Non-PII)’까지도 그 대상에 포함된다. 문제의 핵심은 비식별정보에 관한 부분이다. 빅데이터가 눈독을 들이고 있는 것이 주로 비식별정보이기 때문이다. 따라서 동법이 괄호안의 비식별정보를 개인정보에 포함하고 있는 한 빅데이터 환경에서 수집 및 재가공되는 모든 정보도 동법의 보호대상에 해당하게 되고, 이런 상황은 곧 빅데이터 환경의 컨셉과 정면으로 충돌한다. 이런 이유로 수정담론은 앞서 살핀 바와 같이, 개인정보의 개념을 축소하고자 하는 논의를 진행중에 있다. 즉 비식별정보를 개인식별정보와는 차별적으로 취급을 하여, 그 보호의 수준을 달리하거나 아예 보호의 대상에서 제외하자는 것이다. 특히 ‘다른 정보와 쉽게 결합하여’라는 법문의 해석이 쟁점이다. 비식별정보는 원칙적으로 개인정보에 해당하지 않으나, 바로 이 부분의 해석을 넓게 해석한다면 빅데이터 환경에서 유통되는 일반적인 정보의 대부분이 보호대상인 개인정보의 개념에 포함되게 된다는 것이다.[38] 실제 사례로 방송통신위원회가 발간한 ‘정보통신서비스 제공자를 위한 개인정보보호 가이드’의 내용[39]과 하급심 판결(서울중앙지방법원 2011.2.23. 선고 2010고단5343 판결)의 판시내용[40]을 들고 있다.

한편 빅데이터의 특유한 속성인 다면성(변화가능성)을 지적하기도 한다. 빅데이터 환경에서는 수집된 데이터의 재가공 이전에는 개인식별성을 갖추지 아니하던 것이 재가공 이후에 식별이 가능해질 수도 있는데, 이럴 경우는 도대체 어떻게 대응해야 하느냐 하는 문제가 그것이다.[41] 즉 수집의 단계에서는 개인정보에 해당하지 않았는데, 이용 또는 제공 등의 단계에서는 개인정보에 해당하는 경우가 발생하고 현행 법제에서는 이를 해결해낼 방도가 없다는 것이다.

1.2.2. 비판적 검토

먼저 개인정보의 범위축소와 관련하여 살펴보기로 한다. 앞서 살핀바와 같이 빅데이터 환경이 프라이버시보호에 취약하다는 것은 거의 공인된 바와 다름없다. 이러한 배경위에서 종래의 보호 장치를 허물어내기 위한 입론을 하는 것은 상당히 특이한 발상이라고 평가하면서 이야기를 시작하고 싶다. 왜냐하면 국제적 동향에 비추어 보아도 이러한 발상은 아마도 유일무이할 것이기 때문이다. 예를 들어, 앞서 살핀바 있는 ‘EU 데이터 보호규정안(2012)’의 경우에는 종래의 지침에 비해 개인

38) 박광배, “개인정보 국외이전의 실무적 문제와 개선방향”, 개인정보보호법제 개선 토론회Ⅱ: 개인정보보호 그 현실속으로(프라이버시 정책연구 포럼, 2013), 23쪽.

39) “개인과 관련된 일반적인 정보들은 대부분 다른 정보와 결합하면 개인식별이 가능해지므로 정보통신망법의 적용을 받는 사업자들은 해당 서비스 이용자와 관련된 모든 정보를 개인정보로 간주하고, (이하 중략)” : 박광배, 앞의 글, 23쪽.

40) “당해 정보와 결합 가능한 다른 정보가 모두 동일인에게 보유되고 있는 것을 전제로 하고 있지 아니하고, 쉽게 다른 정보를 구한다는 의미가 아니라, 구하기 쉬운지 어려운 지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정개인을 알아볼 수 있게 되는 것을 말한다”고 판시하였다. 즉, IMEI(국제 모바일 단말기 인증번호)나 USIM 일련번호는 통신사의 데이터베이스에서 관리되어 있고, 그 시스템을 이용하면 누구인지 식별가능하다는 이유로 “쉽게 결합하여“ 개인을 식별할 수 있으므로 개인정보에 해당한다는 입장이다: 박광배, 앞의 글, 23쪽.

41) 최경진/정준현/구태언/지성우/김도승/성준호, 앞의 보고서, 78-80쪽.

정보의 개념을 더욱 확장하여 ‘개인에 관한 모든 정보’라고 규정한 바 있다.[42] 또한 개인에 대한 ‘프로파일링 거부권’을 마련하기도 하였다. 즉 개인적 특성의 평가, 개인에 관한 분석 또는 예측을 위한 기준의 적용을 받지 않는 권리를 보장하고 있는 것이다.[43] 나아가 지난해 오바마 정부가 마련한 ‘소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)’에서는 일종의 ‘프라이버시 보호 기대권’을 정보주체에게 부여하기도 하였다.[44] 이러한 외국의 사례들을 고려해 볼 때, 빅데이터 시대에 즈음하여 개인식별정보만을 보호의 대상으로 하자거나 비식별정보에 대한 보호수준을 축소하자는 것은, 참으로 시대조류에 역행하는 일이 아닐 수 없다.

한편 대다수의 법률에 등장하는 정의규정들이 대체로 그러하듯, 개인정보 개념을 규정하고 있는 동법의 표현 또한 다소 포괄적이고 모호한 면이 있다는 것은 분명하다. 그러나 이는 구체적인 사회현상을 추상적인 언어적 표현 안으로 담아낼 때 필연적으로 발생하는 것이며, 동법상의 정의규정 또한 ‘불명확개념으로서의 오류’ 범위 내에서 작동하고 있다고 평가해야 한다. 따라서 큰 문제는 없다고 할 것이다.

---

42) Article 4, (2): ‘personal data’ means any information relating to a data subject; 그렇다고 말 그대로의 모든 정보를 의미하는 것은 아니며, Article 4, (1)의 ‘data subject’의 정의에서 정보주체의 개념을 한정하면서 이러한 오류를 회피하는 방식을 취하고 있다('data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person).

43) Article 4, 1: Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

44) 3. RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

〈표1〉 개인정보 정의조항 관련 입법례

국 가	내 용
OECD 가이드라인	– 식별되거나 식별될 수 있는 개인에 관한 모든 정보[45]
EU지침	– 식별되거나 식별될 수 있는 자연인에 관한 모든 정보 ; 식별될 수 있는 자란 신원확인번호나 개인이 가지는 고유한 신체적·생리적·정신적·경제적·문화적·사회적 특질 중 하나 이상의 요소 등을 참고(reference)함으로써 직·간접적으로 신원이 확인될 수 있는 사람을 말한다.[46]
EU규정(안)	– '정보주체'란 식별된 자연인 또는 개인정보처리자 또는 다른 자에 의하여 합리적으로 사용될 것으로 보이는, 특히 식별번호, 위치정보, 온라인 식별자 또는 개인의 신체적, 생리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 관한 하나 또는 복수의 요소에 관한 정보들에 의하여 직접적 또는 간접적으로 식별된 자연인을 말한다.[47]; – '개인정보'란 정보주체에 관한 어떠한 정보를 말한다.
영국	– 다음으로부터 식별할 수 있는 생존하는 개인에 관한 데이터 당해 정보; 또는 정보관리자(data controller)가 보유하고 있거나 보유할 가능성(likely)이 있는 기타 데이터나 정보(information). 그리고 해당 개인에 대한 견해의 표시나 해당 개인에 대한 정보관리자 또는 기타 사람들의 의도를 드러내는 모든 표시를 포함하는 데이터나 정보[48]
독일	– 식별되거나 식별될 수 있는 개인의 인적, 물적 환경에 관한 일체의 정보[49]
일본	– 생존하는 개인에 관한 정보로서, 당해 정보에 포함되는 성명, 생년월일 기타 서술 등에 의해 특정한 개인을 식별하는 일이 가능한 것(다른 정보와 용이하게 조합되어, 그에 의해 특정한 개인을 식별하는 일이 가능하게 되는 것을 포함한다)을 말함[50]
미국	– 행정기관이 보유하는 개인에 관한 정보의 개개 항목 또는 그 집합을 말한다. 그 기록(record)에는 당해 개인의 교육, 금전적 거래, 병력, 전과, 취업경력에 관한 정보가 담기지만 이에 한정되지 않는다. 그리고 그 기록에는 당해 개인의 이름 또는 식별번호나 식별부호 혹은 지문, 성문, 사진과 같은 당해 개인에게 고유한 식별자가 포함되어 있어야 한다[51]

45) any information relating to an identified or identifiable individual: 구태언 "개인정보 관련 법령의 문제점과 개선방안", 개인정보보호법제 개선 토론회 II: 개인정보보호 그 현실속으로(프라이버시 정책연구포럼, 2013), 각주20 재인용.

46) any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity: 구태언, 앞의 글(각주 45), 각주 21 재인용.

47) 각주 42 참조.

48) data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller: : 구태언, 앞의 글(각주 45), 각주 23 재인용.

49) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener): : 구태언, 앞의 글(각주 45), 각주 24 재인용.

50) この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）をいう: 구태언, 앞의 글(각주 45), 각주 25 재인용.

외국의 입법례를 살펴보아도 이러한 상황은 크게 다르지 않다. 대부분 유사한 표현을 사용하고 있으며, 다소의 차이가 있기는 하겠으나 해석상 모호한 지점은 분명히 존재하고 있다. 아래의 표[52]를 살펴보기로 하자.

이러한 점들을 종합해 보면 빅데이터 환경의 도래를 이유로 하여 개인정보의 개념을 축소하거나 그 보호수준을 낮추고자 하는 담론을 우리나라 이외에서는 찾아보기 힘들고, 종래 우리나라의 개인정보의 개념설정이 다른나라의 입법례에 비해 턱없이 요상한 바도 없다. 결국 수정담론의 발상은 그리 타당하지 못하다는 것으로 추론해 볼 수 있다.

그렇다면 무한정으로 확대해석할 수 있는 당해 규정의 해석은 어떻게 해결할 것인가? 또한 빅테이터의 다면적 특성으로 인해 새로이 발생하는 문제점은 어떤 방식으로 규제할 것인가 하는 문제가 남는다. 결국 이는 개념규정 자체의 문제가 아니라 동 규정의 해석을 통해 해결해야 할 문제이다. 즉, 주지하는 바와 같이 성문법주의를 취하고 있는 우리나라의 법체제 하에서는 사법부의 융통성 있는 해석을 통해 얻어내어야 할 사항인 것이다. 따라서 방송통신위원회의 유권해석이나 앞서 언급한 하급심의 '다른 정보와 쉽게 결합하여'라는 부분에 대한 해석은, 앞으로 빅데이터 환경아래에서 매우 탄력적인 형태로 변모해 나아가야 할 것이다. 예를 들어 반정형·비정형 데이터의 특성에 부합하는 해석을 지향한다든지, 지금까지 미처 고려하지 못했던 '쿠키(Cookie)' 정보 등 기술적 요소에 대한 입법[53]의 흠결을 보완한다든지 하는 것들을 예로 들 수 있겠다. 요컨대 수정담론이 제시하는 개념규정과 관련한 제문제들은 빅데이터의 특성을 반영하면서도 동시에 우리나라의 프라이버시 정책에 정합성을 가진 해석을 통하여 해결할 것이지, 개념규정의 손질을 통해 해결할 사항은 아니다. 병충해가 예상된다고 하여, 애써 심었던 사과나무를 몽땅 뽑아버릴 수는 없지 않는가?

2. 정보주체의 동의권 변경론

2.1. 정보주체의 동의권

세계적으로 정보주체의 동의권과 관련하여서는 유럽식의 '옵트인(Opt-in)' 제도와 미국식의 '옵트아웃(Opt-out)' 제도로 대별해 볼 수 있다. 옵트인 제도는 개인

51) 5 U.S.C. §552a (a) (4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph: 구태언, 앞의 글(각주 45), 각주 26 재인용.

52) 이 표는 구태언, 앞의 글(각주 45), 35-36쪽에 나오는 표를 그대로 인용하였다.

53) 2009년 개정된 ePrivacy Directive, 즉 'DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)'에서는 쿠키정보의 수집을 제한한 바 있다.

정보를 수집·처리하기 이전에 미리 정보주체에게 수집과 처리의 목적을 고지하고 정보주체의 명시적인 동의(Affirmative authorization)를 받아내는 제도를 말한다. 한편 옵트아웃은 우편, 전자우편, 브로슈어, 팝업, 인터넷 알림 등을 통하여 정보주체에게 개인정보의 수집·처리를 알리고 이에 대해 정보주체가 정식(formally)으로 이의를 제기하지 않으면 개인정보를 처리할 수 있도록 하는 제도를 말한다.[54]

이러한 구분에 의하면 우리의 개인정보 보호법제는 원칙적으로 옵트인 제도를 채택하고 있으면서, 아주 예외적으로 옵트아웃을 병행하고 있는 것으로 판단해 볼 수 있다. 즉 개인정보보호법에 의하면 개인정보의 수집시(동법 제15조 제1항)·제3자 제공시(동법 제17조 제1항)·국외 제3자 제공시(동법 제17조 제3항)·목적 외의 이용시(동법 제18조 제2항)·제공받은 자의 목적 외의 이용시(동법 제19조) 등 개인정보의 수집·처리와 관련한 대표적인 경우에 정보주체의 동의(즉 옵트인)를 얻도록 규제하고 있다. 그 동의의 방법으로는, 각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고, 이를 통해 각각 동의를 받아야 한다(동법 제22조 및 동법 시행령 제17조). 이러한 동의절차는 일종의 개인정보 보호법제의 대원칙으로 기능하고 있기 때문에, 기타 관련법규에서도 그 내용은 동일한 상황이다. 다만 특이하다고 할 수 있는 다음의 몇 가지의 경우를 제외하고 말이다. 먼저 개인정보보호법상의 '민감정보'와 '고유식별정보'의 경우에는 '별도의 동의'를 구해야 한다(동법 제23조 및 제24조). 이는 정보통신망법상의 '구분동의'(동법 제24조의2 제3항)와 일맥상통한 취지이라고 할 수 있다. 다음으로 '신용정보의 이용 및 보호에 관한 법률'에서 등장하는 '서면주의의 원칙'(동법 제32조 제1항 제1호)이 독특하고, 위치정보보호법에서는 미리 약관상에 명시한 이후에 동의를 얻도록 하고 있는 점(동법 제18조 제1항)이 특이하다.

한편 옵트아웃을 허용하고 있는 예외적인 경우를 들자면, 개인정보보호법 제27조의 '영업양도 등에 따른 개인정보의 이전 제한'의 경우와 위치정보보호법 제22조의 '사업의 양도 등의 통지'의 경우가 있다. 나아가 아예 동의가 배제되는 경우도 있다. '정보주체로부터 별도의 동의를 받은 경우', '다른 법률에 특별한 규정이 있는 경우', '정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명· 신체·재산의 이익을 위하여 필요하다고 인정되는 경우', '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우', '개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우', '조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우', '범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우', '법원의 재판업무 수행을 위하여 필요한 경우', '형(刑) 및 감호, 보호처분의 집행을 위하여 필요한

54) 이창범, 앞의 글, 519-520쪽.

경우’ 등(개인정보보호법 제18조 제2항)이 그것이다.

2.2. 수정담론의 논지

이 부분과 관련하여 수정담론은, 개인정보자기결정권이 잘못 해석되고 있다는 논지를 바탕으로 정보주체의 동의권과 관련된 논의를 시작하고 있다. 즉 개인정보자기결정권을 사회적 인격상에 관한 자기결정권의 핵심 내용으로 본다면, 개인정보자기결정권의 본질은 개인정보의 ‘공개’에 있는 것이지 개인정보의 ‘수집’에 있는 것이 아니라는 것이 핵심이다.[55] 나아가 개인정보자기결정권은 기본적으로 ‘대국가적’ 권리이기 때문에, 사인간의 관계에 있어서는 전면적으로 적용될 수 없고 그 판단기준이 달라져야 함을 주장[56]하기도 한다. 또한 개인정보자기결정권이 가지는 포괄성 때문에 실제 그 적용에 있어서는 무력한 것[57]이며, 이러한 문제를 해결하기 위해서는 공공부문과 민간부문의 차별화[58]는 물론 사생활영역과 공개영역의 구분이 전제되어야 한다[59]라는 논지를 펴고 있다. 이는 개인정보자기결정권 개념설정상의 오류를 지적하는 것이거나 최소한 개념상의 변화가 필요하다는 주장으로 이해할 수 있다.

이러한 바탕위에서 수정담론은, 정보주체의 동의를 전제로 하고 있는 현행 개인정보 보호법제가 ‘과도하게 엄격함’을 주장한다. ① 정보의 국외이전 등의 경우에, 수만 명에 이르는 고객들로부터 일일이 동의를 받아낸다는 것이 현실적이지 않다는 점, ② 실제 개인정보 이전 등의 경우에 정보주체가 관심을 두지 않은 경우가 많고, 관심이 있다하더라도 대체로 무감각한 동의에 불과할 것이라는 점, ③ 정보주체의 동의를 받아야 이전을 할 수 있다는 것은 정보주체의 동의만 있으면 이전을 할 수 있다는 일종의 ‘사업자 면책규정’으로 악용될 우려가 있다는 점 등을 근거로 논하고 있다.[60]

한편 빅데이터의 속성상, 이러한 동의제도가 매우 부적합하다는 주장도 있다. ① 빅데이터는 수집된 데이터의 자유로운 조합과 연결을 전제로 있어 서로 다른 영역에서 발생한 데이터들과의 결합이 필수적이므로, 데이터의 결합과정에 대한 규제가 최소화되고 자유로운 결합이 인정되어야만 새로운 가치창출이 가능하다는 것이 주요한 논지이다. 또한 ② 정보주체가 그 자체로서는 식별성이 없는 정보에 대하여 추후의 결합여부나 결합범위를 미리 결정·선택하게 한다면 이는 결국 각 정보주체마다 그 결합의 정도를 따로 따로 정해야 한다는 것인데, 이럴 경우 증가하게 되는 결합·유지비용 때문에 빅데이터의 실현이 사실상 불가능하다는 것도 유력한 근거로 들고 있다. 나아가 ③ 빅데이터의 속성상 새로운 정보의 생성시점이나 그 내용상의

55) 문제완, 앞의 글, 9쪽.
56) 구태언, 앞의 기고문, 2쪽.
57) 문제완, 앞의 글, 9-10쪽.
58) 구태언, 앞의 기고문, 2쪽; 문제완, 앞의 글, 10쪽.
59) 문제완, 앞의 글, 10쪽.
60) 박광배, 앞의 글, 29-30쪽.

범위를 특정한다는 것이 곤란하므로, 개인정보의 ‘수집시의 동의’는 몰라도(개인정보보호법 제15조) ‘처리에 관한 동의’를 선택·결정할 권리(개인정보보호법 제4조 제2호)는 실현하기가 곤란하다는 점도 부적합의 좋은 사례로 예시하고 있다.[61]

이러한 점들을 이유로 하여 수정담론은, ① 기존의 고지와 동의 일변도의 규제정책에서 탈피하여 정보주체에게 요구되는 고지와 동의사항을 정보주체가 실질적으로 예측하기 어려운 경우로만 한정하는 방향으로 법률을 개정[62]해야 한다거나 ② 빅데이터와 관련한 동의의 방식을 옵트아웃으로 전환하자는 주장[63]을 그 해결책으로 제시하고 있다.

2.3. 비판적 검토

먼저 ‘개인정보자기결정권의 해석상 오류’를 주장하고 있는 첫 번째 논지에 대해 살핀다. 개인정보자기결정권의 본질이 개인정보의 ‘공개’에 있는 것이지 개인정보의 ‘수집’에 있는 것이 아니라는 주장은 참으로 어처구니가 없다. 개인정보가 공개되지 않은 채로 무한정 수집만 된다고 가정한다면, 자기결정권과는 전혀 무관하고 정보주체의 기본권이 보장된다는 것인가? 또한 개인정보자기결정권이 기본적으로 ‘대국가적’ 권리이기 때문에, 사인간의 관계에 있어서는 전면적으로 적용될 수 없다는 부분도 마찬가지이다. 한 개인이 헌법에 의해 부여받는 기본권에 대한 해석을 어찌 이런 식으로 할 수 있단 말인가? 아주 쉬운 예를 들어보자. 신체의 자유권이라는 기본권은 국가가 특정인을 체포할 때에만 적용되고 사인이 타인을 감금하거나 체포할 때에는 적용되지 않는다는 것인가? 이러한 점에서 당해 논지는, 전반적으로 개인정보자기결정권에 대한 이해가 부족하거나 판단상의 오류에서 비롯된 것이 아닌가 한다. 지면의 관계상 이를 상술할 수는 없겠으나, 어찌되었건 우리 헌법상의 개인정보자기결정권은 그러한 것이 아니며 앞으로 그리 변해서도 안 된다는 점은 분명하게 해두고 싶다. 나아가 공공부문과 민간부문의 차별화는 물론 사생활영역과 공개영역의 구분이 전제되어야 한다는 논지도 이상하기는 마찬가지이다. 주지하는 바와 같이 현행 개인정보보호법은, 공공부문에 관한 보호법제만이 존재하여 민간부문에 대해서는 긴 시간동안 입법공백의 상태였던 것을 해결해낸 장본인이다. 즉 그 부문에 있어 공공과 민간을 구분하지 않고 보편·타당하게 적용될 수 있는, 개인정보에 관한한 모법의 의미를 가지는 것이 바로 동법의 입법취지이다. 이러한 연혁을 거슬러, 다시금 그 부문을 나누어 규제해야 한다는 주장이 도대체 얼마나 정합성을 가지고 있는 것인지 가늠하기 힘들다.

다음으로 정보주체의 동의를 전제로 하고 있는 현행 개인정보 보호법제가 ‘과도하게 엄격’하다는 주장에 대해 살핀다. 옵트인 제도자체를 엄격하다는 판단의 기준으로 삼고 있는 것인지는 불분명하나, 만약 그러한 취지이라면 우리보다 훨씬 더

61) 최경진/정준현/구태언/지성우/김도승/성준호, 앞의 보고서, 81-82쪽.
62) 박광배, 앞의 글 30-32쪽.
63) 박광배, 앞의 글, 32쪽; 최경진/정준현/구태언/지성우/김도승/성준호, 앞의 보고서, 82쪽.

과도하게 엄격한 국가는 유럽에 너무나 많다. 앞서 살핀 바와 같이, 유럽의 개인정보 보호법제 또한 우리와 마찬가지로 옵트인 방식을 채택하고 있으며, 규제의 강도나 규정내용의 섬세함에서는 이제 막 걸음마를 떼고 있는 우리의 법제와는 그 차원을 달리한다고 말할 수 있다. 유럽의 경우에도 어김없이 빅데이터의 시대가 도래할 것이 자명한데, 그럼에도 불구하고 현재의 유럽은 기존의 규정에다 한층더 강화된 입법을 열심히 지원하고 있다. 일일이 동의를 받아낸다는 것이 현실적이지 않다는 점, 실제 정보주체가 이에 무관심하다는 점, 동의제도가 사업자 면책규정으로 악용될 여지가 있다는 점 등의 문제들도 우리나라나의 상황과 크게 다르지 않을 것이다. 다만 이러한 문제를 해결하는 방식으로, 유럽은 좀 더 세밀하고 한층 강화된 입법을 선택한 것뿐이다. 즉 '과도하게 엄격'하여 발생한다는 문제들에 대하여, 더욱 정합성을 가진 입법적 조치를 강구함으로써 해결해야 할 일이지 기존의 입법내용마저 허물어낸다면 점점 더 미궁으로 빠져드는 것이 아닐지 생각해 보게 된다.

마지막으로 빅데이터의 속성상 현행의 동의제도가 부적합하다는 논지에 대하여 살핀다. 예시한 3가지의 논거를 살피는 동시에 앞서 살펴본 바 있는 빅데이터의 특성을 고려할 때, 이 논지는 상당부분 타당한 주장이라고 할 수 있다. 그러나 그 해결을 위하여 기존의 옵트인 체제를 허물어내고 옵트아웃으로의 대전환이 필요하다는 결론에는 동의할 수 없다. 왜냐하면 이 문제는 동의제도 자체의 문제이라기보다는 새로운 형태의 기술적 특성이 빚어낸 입법부조화의 문제이기 때문이다. 이러한 입법부조화는 정보통신 관련법규에는 빈번히 출현하는 문제이다. 기술의 발전속도를 법제가 따라가지 못하는 것은 어찌보면 너무나 당연한 것이기도 하다. 통상 이러한 난관의 해결은 기술발전의 추이를 신중하게 짚어보고 이를 수용할 것인지의 여부를 결정하는 입법자의 면밀한 판단 이후에 수정 및 보완되는 것이 일반적이다. 따라서 그 도래가 임박한 지금의 시점이 아니라, 본격적으로 빅데이터 환경이 도래하고 난 이후에나 판단해야 할 문제인 것이다.

한편 필자는 이 논지와 관련하여 반드시 적시하고 싶은 한 가지가 있다. 만약 이러한 부조화를 이유로 진정 개인정보보호의 패러다임이 변해야 한다면, 그것은 바로 개인데이터의 '수집'을 통제하는 것에 많은 배려를 하고 있는 현재의 개인정보보호법 체제가 데이터의 '생산'이나 '사용'에 더 많은 초점을 맞추도록 조율하는 작업이 되어야 한다는 점이다. 현행의 규정은 어디까지나 정보주체와 이를 수집하는 기업 간의 관계를 설정하고자 하는 1차원적 접근을 토대로 하고 있고, 그 수집된 정보가 유통되거나 새로이 가공되는 등의 다차원적인 시각에 있어서는 상대적으로 부족한 배려에 그치고 있는 것이 사실이다. 특히 빅데이터 환경의 속성상 수집된 정보의 이동과 변모는 가히 극한에 달할 것이 자명하게 예상되는 바이므로, 데이터의 흐름을 다면적·다층적 견지에서 바라본 규정의 신설이 필요할 것이다. 다만 이러한 수정작업이 현행의 동의제도나 수집단계에 대한 원칙들을 부정하면서 진행되어져서는 곤란하다. 왜냐하면 아무리 급속한 기술발전이 발생한다고 하여도, 정보주체와 그의 데이터를 최초로 수집하는 주체는 항상 존재해야 하기 때문이다. 즉

현재의 규정내용은 말 그대로 기본이자 원칙이기 때문에, 필요에 의한 부정이 있을 수 없다. 요컨대 개인데이터 자체에 대해 주력하고 있는 현재의 초점에 더하여, 앞으로는 개인데이터의 가공과 활용에도 더 많은 주목을 해야 한다는 것이다.

Ⅳ. 나오며

지금까지 우리는 빅데이터 환경에서 예상되는 새로운 변화들과 이에 대한 여러 법적 이슈들을 검토해 보았다. 앞서 살핀 바와 같이, ICT 기술의 눈부신 발전이 새로운 디지털 시대의 개막을 견인해내는 저력을 보이고 있는 것은 분명한 것 같다. 또한 이러한 변화덕분에 새로이 발생되는 문제점들도 그리 호락호락하지 않음을 확인해 보기도 하였다. 그러나 수정담론이 제시하고 있는 각종 대안이나 해결책들이 그다지 타당하지만은 않다는 검토의 결과를 말하게 되어 매우 유감스럽기도 하다. 너무 성급하거나 매우 위험한 생각들을 포함하고 있다는 인상을 지울 수가 없었기 때문이다. 아직은 추상적인 상황에 불과한 빅데이터 환경을 위하여, 수많은 시간과 노력을 통해 가꾸어온 우리의 입법과 원칙들을 짧은 순간에 허물어낸다는 것이 얼마나 허망한 일인가?

돌이켜보면, 인류의 역사는 마치 탑을 쌓아올리듯 진행되어 왔다. 노력과 경험을 통해 얻어낸 기존의 진리를 토대로 삼아, 다시금 새로운 도전과 반성을 담은 또 다른 한 층을 올리는 방식이 그것이다. 그런 의미에서 진보는 경험에 대한 반성이며, 창조는 지식에 대한 존경에서 비롯된다. 이에 대입하자면, 지금의 시점은 새로운 한 층으로의 도약을 꿈꾸는 시기일 뿐 개인정보 보호체제의 패러다임적 전환 시기로는 너무 이르다.

아직은 반성과 보완의 시점인 것이다.

빅데이터 환경과 개인정보의 보호방안

— 개인정보 보호법제 수정담론에 대한 비판적 검토 —

오 길 영

불과 수년전의 우리는, ‘디지털(Digital) 혁명’이라는 표제에 고개를 끄덕인 바 있다. PC와 노트북을 통한 인터넷 접속과 이메일의 사용, 디지털 이미지와 MP3 음원 등 새로운 컨텐츠의 보급은 가히 가공할 만한 변화를 우리의 생활 속에 가져다 주었다. 한편 지금 이시간의 우리는, 또다시 새로운 국면을 맞이하고 있다. 기기와 매체 중심적이던 디지털 혁명의 초기적 환경은 이제 점차 네트워크를 보편적 기반으로 하는 새로운 형태로 변모해 가고 있는 것이다.

이러한 면모는 새로운 ICT 환경의 도래와 새로운 사회적 이슈가 발생하고 있음을 의미한다. 최근의 예를 들어 보자면, 소위 ‘빅데이터(Big Data)’ 열풍이 가장 대표적이다. 인류의 수많은 디지털 활동이 양산해내는 방대한 양의 데이터들을 새로이 가공하여 상품화할 수 있는 새로운 ICT 환경에 대하여, 지금 전세계 인터넷산업의 시선이 여기에 쏠려 있다고 해도 과언이 아니다. 이러한 빅데이터 환경의 시작에 발맞추어, 현재 학계에서도 개인정보 보호정책에 대한 대대적인 수정담론이 연이어 등장하고 있다. 현행 개인정보보호법의 개정 필요성을 주장함은 물론 법제 자체를 관통하는 대원칙에 대한 본격적인 비판이 시작된 것이다.

이 글은 최근 이러한 논의들의 타당성에 대한 의문을 제기하면서 시작되었다. 빅데이터 환경의 새로운 가능성에 대한 흥분의 시선만이 존재하는 것은 아니기 때문이다. 빅데이터 환경이 불러오는 부작용, 즉 ‘네트워크 프라이버시의 침해’ 또는 ‘개인정보의 사회적 해킹’ 등으로 표현되는 거대한 역기능에 대한 우려가 공론화되어가고 있는 국제적인 움직임 또한 주의 깊게 관찰해야 한다. 이 글은 이러한 관점을 바탕으로, 개인정보 보호법제에 대한 수정담론을 비판적 시각에서 검토하는 것을 주요한 내용으로 한다. 빅데이터 환경에 대한 간략한 개관과 이로 인해 발생하는 새로운 법적 이슈들을 요약해보고, 이에 대하여 개인정보 보호법제의 총체적인 수정으로 대응하고자 하는 신생 담론들을 비판적 시각에서 분석하는 것이 이 글의 목적이다. 특히 빅데이터 환경하의 정보주체의 관점에서, ‘개인정보의 개념 재설정’과 ‘동의권의 재구성’ 논의에 대한 구체적인 타당성을 검증하는 것에 초점을 맞추고 있다.

주제어: 개인정보보호, 개인정보자기결정권, 빅데이터, 옵트인, 옵트아웃

제6주제

유럽 개인정보보호 개정이 시민에게 미치는 영향 : 어떤 선택을 할 것인가

The Impact of the European Data Protection Reform on Citizens Which Choices Remain?

Janneke Slöetjes*

Introduction

European laws that protect the personal data and privacy of citizens have always ranked amongst the highest developed data protection laws in the world. In January 2012, the European Commission (EC) has launched a reform of these rules, introducing a draft Data Protection Regulation (the 'Draft Regulation) which has channelled a very fierce debate about the future of data protection and privacy. The draft tries to accommodate new technologies and provide security and choice for both citizens and businesses - but will it do what it promises?

The reform of the European Framework attracts a lot of attention, not only within Europe, but from all over the world. The European debate is likely to shape future data protection law on a very big scale, as many countries aim to achieve maximum interoperability with the European framework. Also, many laws throughout the world are based on the European standards, so it can be expected that new European changes will lead to changes to for instance Latin-American data protection laws.

Contents of this paper

This paper aims to provide you with an outline of European data protection law and the changes presented in the Draft Regulations. This paper will firstly explore the current rules in short and comment on the background of the current law and the need for new legislation. Secondly, it will describe the most interesting features of the new Draft Regulation. Finally, the paper will describe the political state of play: which forces influence the reform and what are possible outcomes?

* 비츠 오브 프리덤 변호사, 네덜란드

Overview

I. The Current European Data Protection Framework

European data protection laws were harmonized for the first time in 1998, when the European Data Protection Directive (95/46/EC, hereinafter referred to as 'the Directive')[1] was implemented in the laws of the European Member States. Prior to this Directive, each European Member States had its own data protection law. The Directive is built upon the 1980 OECD Guidelines and consists of data protection principles regarding transparency, legitimate purpose and proportionality. These principles can also be found in South-Korea's PIPA law of 2011.

The current framework is based upon the following principles.

1. *Information and access (articles 10, 11, 12).* The data subject has the right to be informed when his personal data is being processed. The party responsible for the processing (data controller) must provide its name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. The data subject also has the right to access all data processed about him, as well as a right to demand rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12)

2. *Legal basis (article 7).* Data processing should always be based on one out of six legal grounds. Data can be processed when

1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- consent has been obtained; or
- processing is necessary for the performance of or the entering into a contract; or
- processing is necessary for compliance with a legal obligation; or
- processing is necessary in order to protect vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

3. *Legitimate purpose (art. 6 b).* Personal data may only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.

4. *Proportionality (article 6).* Personal data may be processed only insofar the data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must furthermore be accurate and up to date and should not be kept in a form which permits identification of data subjects for longer than necessary.

5. *Sensitive data (article 8).* When sensitive personal data, such as religious beliefs, political opinions, health, sexual orientation, race, or trade union membership, are being processed, stricter rules apply.

6. *Right to object (article 14).* The data subject may object at any time to the processing of personal data for the purpose of direct marketing.

7. *Automated decision making (article 15).* Decisions which produce legal effects or significantly affect a data subject may not be based solely on automated processing of data. A form of appeal should be provided when automatic decision making processes are used.

II. The need for new legislation: what is lacking in Europe?

1. Technological Changes

The changes proposed by the European Commission are heavily influenced by technological changes. The rise in electronic processing, the growth of online services and the fact that the amount of personal data is and will continue to rise strongly has obviously inspired a great number of the proposed changes to the law. The European Commission strives to protect personal data better in an online environment and to give citizens more control over their data.

2. Economic Growth in Europe

The European Commission wants to streamline the laws for the private sector in order to make it easier for companies to do business in Europe. Replacing 27 different data protection laws with one Regulation makes it easier for businesses to comply. Also, certain administrative requirements, such as notifying processing operations to Data Protection Authorities (hereinafter also referred to as DPA's) will be abolished.

3. Enforcement and Sanctions

Enforcement of data protection laws throughout Europe has never been consistently strong. Some Data Protection Authorities are relatively powerful and strong, while others are severely understaffed. Understaffed DPA's cannot enforce data protection law adequately. Another issue related to enforcement is that the maximum sanctions are very low in some Member States. For example, the maximum sanction for a breach of certain administrative requirements related to data protection in the Netherlands is EUR 4,500 (6.500.000 South-Korean Won). DPA's do have the power to investigate companies or governmental organizations which are suspected to breach of data protection law. When establishing such a breach, a DPA may impose a high penalty during the period the breach is not remedied. However, such a regime is only successful when DPA's have sufficient time to investigate more than a handful of cases per year.

4. Open Norms

Finally, the abovementioned data protection principles are mainly open norms. This makes them flexible and allows them to apply in a multitude of situations and across both the private and the public sector. On the other hands, the openness causes vagueness and uncertainty. Also, many terms have been interpreted somewhat differently across Member States. The European legislator has trusted these open norms to be filled in by case law. However, there have not been many court cases on data protection related issues. Court cases relating to privacy and data protection are often handled based on articles 7 and 8 of the European Charter of Human rights or article 8 of the European Convention of Human Rights. These articles protect the private lives of individuals as well as the right of protection of personal data. For the most part, companies confronted with data protection requirements have a hard time to figure out what exactly open norms such as 'adequacy' or 'legitimate interest' mean in practice. The European Commission tries to fill in more details in the current law, clarifying some legal concepts.

III. Changes Proposed by the Draft Regulation

The European Commission has put forward a proposal[2] for new data protection rules in January 2012, announcing an update to the data protection framework. Firstly, it wants to change the legal structure of the law from a Directive to a Regulation. A regulation will be directly applicable and enforceable in all European Member States, which means the law will be exactly the same throughout Europe. This is advantage for businesses, as they no longer will have to comply with a patchwork of different rules.

Secondly, the European Commission has proposed a number of interesting updates to the existing regime. These updates are intended to decrease the number of administrative sanctions for data controllers (companies as well as governmental organizations that process personal data) as well as to provide more

2) 25 January 2012, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COD) 2012/0011.

control and transparency to data subjects (the citizens whose personal data are being processed).

What's in it for citizens?

Hereinafter is an overview of the most interesting new provisions in the Draft Regulation that are intended to award citizens better protection of their personal data.

A better definition of protected data (article 4(1) Draft Regulation)

The European Commission proposes a small change to the definition of 'personal data' by clearly stating that online identifiers such as device numbers, IP addresses or cookie identifiers can identify a natural person. As such, such data fall under the scope of the Draft Regulation and are protected.

Stricter rules for consent (article 7 Draft Regulation)

The European Commission proposes to change the consent requirement from regular consent to 'explicit consent'. This means that when a data controller wants to obtain consent from a citizen, it has to ask explicitly whether a person consents to the use of its personal data for a specific purpose. This is specifically intended to give citizens more control over their data and to prevent situations where consent is 'hidden' in general terms and conditions.

Secondly, it means that consent cannot be considered obtained validly when there is a significant imbalance between the data controller requesting the consent and the data subject (citizen). A doctor can therefore not base processing of personal data on consent, and neither can an employer. Such parties need to find another legal ground as the basis for data processing.

A right to be forgotten (article 17 Draft Regulation)

One of the most controversial additions to the Draft regulation is the so-called "right to be forgotten". This is in the first place due to the quite controversial title: contrary to what it claims, it does not imply a full right for citizens to have their data erased under all circumstances. The provision is however quite badly drafted and as a result hard to understand. This has raised severe worries about the exact scope of the provision, and led to a debate regarding possible infringments of the right to free speech.[3)]

3) See for instance http://techliberation.com/2010/11/05/the-conflict-between-a-right-to-be-forgotten-speech-press-freedoms/

The European Commission has proposed that every citizen has the right to obtain from the controller the abstention from further dissemination of its personal data. In addition, when a data controller has made personal data public, it should take all reasonable steps

to inform third parties who are processing the data, that the citizen has requested the erasure of the information, of links to the information of of copies of the personal data.

There are a number of exceptions to this right, for instance when retention of the data is necessary for exercising the right to free speech, for public health reasons or for statistical, historical or scientific research purposes. Nevertheless, it is feared that the right to be forgotten in the from proposed by the European Commission will put too much pressure on data controllers to erase data they published and to have it erased by third parties as well.

The right to take your data with you (data portability, article 18 Draft Regulation)

The European Commission introduces an addition to the right to access, erase and correct personal data. Under the draft Regulation, it becomes possible for data subjects to obtain an electronic copy of their personal data, so that they can take their data from one data controller to another if they wish. This new provision is intended to prevent lock-in of customers in for instance social networks. It can however also be of use for other services, as it allows you for instance to port your telecom data to another provider and receive a good new offer based on your exact use, or to track the energy consumption in your household by obtaining an overview that can be analyzed. The big advantage over a mere copy is that it is a digital file, which allows you to analyze the data yourself or upload it to another company of your choice. Next to preventing lock-in, this provision aims to increase competition between services in Europe, as it becomes easier for citizens to move from one service to another when they are dissatisfied.

for an overview of objections raised against the so-called 'right to be forgotten'.

New rules prohibiting profiling (article 20 Draft Regulation)

The current article 15 of the Directive prohibits automated decision making unless a number of criteria are met. For one, automated decisions may not be based solely on sensitive data. There should also be additional safeguards in place, such as information regarding the fact that automated decisionmaking (profiling) takes place and the consequences of such profiling.

Data breaches must be reported to DPA's and citizens (article 31 and 32 Draft Regulation)

The Draft Regulation contains provisions that require data controllers to report data breaches to DPA's as soon as possible (generally within 24 hours). When the breach is likely to affect citizens adversely, the breach must also be reported to them.

A new regime for compliance and higher penalties (article 79 Draft Regulation)

Under the new proposal, Data Protection Authorities from European countries will work closer together in order to bridge the differences between the different authorities. Decisions taken by one of the authorities will be submitted to other authorities as well in order to guarantee consistent enforcement throughout the EU.

Secondly, all DPA's will be granted the same enforcement power, including powerful sanction possibilities. A breach of data protection rules may lead to a fine of 0,5% up to 2% of the company's worldwide global turnover.

IV. Political State of Play

Since the proposal was put forward by the European Commission, both the Council (of Ministers; formed by the Ministers of Justice from each Member State) as well as the European Parliament ("EP") have provided comments and amendments to the draft proposal. The negotiations that take place within the Council are secret, only the outcomes of each round of negotiations are being published. The deliberations of the European Parliament are more public and open. As such, the European Parliament is the place sought out by lobbyists to influence the proposal and convince the Members of European Parliaments (MEPs) to file amendments to alter the proposed Regulation.

1. The Brussels lobby storm

The influence of lobbyists on this particular piece of draft legislation has proven to be very strong. The responsible Commissioner, Ms. Viviane Reding, has declared the lobby around data protection the 'fiercest lobby ever'.[4)]

Internet and IT companies, both American and European, lobby very hard for more flexibility and less rules, as do telecom operators, banks, (online) advertisers, publishing houses and insurers. As a result of heavy lobbying, an astounding total of 4000 amendments has been filed over the course of a little over a year. Research by Austrian activists[5)] has shown that many MEPs copy pasted proposals directly from business lobby briefs. Especially politicians of the conservative European People's Party have used this method to file their amendments to the proposal. Most amendments aim to provide businesses with more flexibility around data processing and greater freedom to store, analyze, use and combine personal data of citizens.

European activists of digital civil rights have of course also lobbied the Parliament but have been outnumbered for the most.

2. European Parliament voting results

Even though the European Parliament has not yet conducted its plenary vote on this issue, there have been three votes in opinion Committees[6)] in the Parliament. The outcome of such opinion votes is a good predictor for what will happen during a plenary vote. It shows clearly that all Committees have favored the interests of businesses over the interests and rights of citizens. This has resulted in changes to many of the proposals that were newly launched by the European Commission. Consent no longer needs to be explicit, data portability should be limited, data breach notification is only necessary in severe cases and the rules to subject people to profiling will become more lenient. Sanctions are being slashed, and MEPs have introduced a special sub-category of personal data (so-called 'pseudonymous data', were a direct identifier is replaced by a pseudonym) that requires less protection, giving companies more freedom to use such data, especially online. Many MEPs also support more flexible rules to export data to

4) http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html

5) See www.lobbyplag.eu for an overview of all amendments and which politicians copypasted most.

6) The involved Opinion Committees are: Internal Market and Consumer Protection (IMCO), Industry, Research and Energy (ITRE) and Legal Affairs (JURI).

third countries, regardless of the level of protection of personal data in these countries, and less strict purpose limitation principles.

3. Next steps

From a civil society point of view, the voting results so far have been very discouraging. Next up will be the vote in the LIBE (Civil Liberties, Justice and Home Affairs) Committee, which is the leading Committee on this file. As such, the responsible Member of Parliament who is also a member of LIBE, will take all results from the previous voting rounds into account and present a full draft package before the vote which is scheduled for 21 October 2013.

Given the previous outcome, such a package cannot contain many positive solutions. However, not only the Parliament, but also the European Commission as well as the Council each have an equal stake in the negotiations before settling on a final text, which then will have to be approved by a majority of the MEPs in a plenary voting session. It seems unlikely that the European Commission will agree to an extremely watered down version of its original proposal.

4. Conclusion: what remains for citizens?

Although it is a bit too early to be totally discouraged, it is very well possible that European citizens will end up with worse data protection law and less protection of privacy than they currently enjoy under the Directive. The European Commission has tried to bring matters forward and modernize data protection law, but its efforts are currently being met with counterproposals that aim to achieve the exact opposite.

This is a rather ironic situation since everyone is well aware that personal data of citizens is very valuable and will continue to play a growing role in our economy and society. Sadly, politicians seem to perceive it not as a fundamental right that deserves protection, but merely as currency for the digital economy.

Abstract

The Impact of the European Data Protection Reform on Citizens Which Choices Remain?

Janneke Slöetjes

European laws that protect the personal data and privacy of citizens have always ranked amongst the highest developed data protection laws in the world. In January 2012, the European Commission (EC) has launched a reform of these rules, introducing a draft Data Protection Regulation (the 'Draft Regulation) which has channelled a very fierce debate about the future of data protection and privacy. The draft tries to accommodate new technologies and provide security and choice for both citizens and businesses – but will it do what it promises?

The European Commission has introduced a number of new concepts to the existing law. These aim to cut costs for businesses and give citizens more control over the use of their personal data. The changes include a better definition of personal data, aiming to protect data better in an online environment, stricter rules for obtaining consent and a so-called right to be forgotten, which allows citizens to have information published about them removed. This new right raises questions with respect to the protection of the right to freedom of speech. Furthermore, the proposal contains the right for citizens to obtain a full electronic copy of their data, rules for data breach notification and higher sanctions for companies and governments that breach data protection laws.

The European Parliament has met the legislative proposal with a storm of counter proposals. Most of these proposals will lead to a decrease of privacy protection as they aim to give businesses more room to process personal data of citizens for their benefit. This is not surprising since a significant number of the proposals and amendments introduced by Members of Parliament came straight from lobbyists proposals.

The outcome of the legislative process is therefore far from certain. Europeans may end up with less protection of their personal data than they currently enjoy.

This paper will analyze the need for an update to data protection law and explore the new additions proposed by the European Commission. Finally, it will explain the political state of play and possible outcomes.

유럽 개인정보보호 개정이 시민에게 미치는 영향 : 어떤 선택을 할 것인가

Janneke Slöetjes*

서론

시민들의 개인 데이터와 프라이버시를 보호하는 유럽 법은 전 세계적으로 항상 최고 수준의 데이터 보호법으로 간주되고 있다. 2012년 1월 유럽집행위원회(EC)는 이러한 규정 개혁안을 발족해 데이터 보호 규정 안(규정 안)을 도입해 향후 데이터 보호 및 프라이버시에 관한 드센 논쟁을 완화시켰다. 이 안은 새로운 기술을 접목시키고 시민과 사업체 둘 모두에 보안과 선택의 여지를 제공해주고자 하고 있다. 하지만 약속한 바를 이룰 수 있을까?

유럽 프레임워크의 개혁은 유럽 내에서 뿐 아니라 전 세계적으로 많은 관심을 집중시켰다. 유럽에서의 논쟁은 많은 국가들이 가능한 유럽 프레임워크와 상호 운영성을 최대한 높이려 하고 있기 때문에 향후 데이터 보호법에 지대한 영향을 미칠 가능성이 높다. 또한 전 세계의 많은 법들이 유럽 기준에 기초하고 있기 때문에 유럽에서의 새로운 변경사항이 예를 들면 라틴 아메리카에서의 데이터 보호법의 변경을 가져오게 될 것이라 예상하고 있다.

논문 목차

본 논문은 유럽의 데이터 보호법을 개관해보고 규정 안에서 제시한 변경 내용을 살펴보기 위한 것이다. 이 논문은 우선 간단하게 현재의 규정을 살펴보고 현 법규의 배경 및 입법 필요성에 대해 간략하게 언급할 것이다. 둘째 본 논문은 새 규정안에 있어 가장 흥미로운 특징들을 기술한다. 마지막으로 본 논문에서는 정치적 활동현황을 기술한다. 즉 어떤 정치적 세력이 개혁에 영향을 미칠 것인가와 가능한 결과는 무엇인가를 기술할 것이다.

* 비츠 오브 프리덤 변호사, 네덜란드

목 차

Ⅰ. 현 유럽 데이터 보호 프레임워크

유럽 데이터 보호법은 1998년 유럽 회원국 법에서 유럽 데이터 보호령(95.46/EC, 이하 '시행령'으로 지칭)[1]을 시행했을 때 처음 선을 보였다. 각 유럽 회원국들은 자체적인 데이터 보호법을 가지고 있었다. 이 시행령은 1980 OECD 지침에 근거해 작성되었고, 투명성에 관한 데이터 보호 원칙, 입법 목적 및 비례원칙(proportionality) 등으로 구성되어 있다. 이러한 원칙들은 또한 남한의 2011년 PIPA법에서도 찾아볼 수 있다.

현 프레임워크는 다음과 같은 원칙에 기초하고 있다

1. *정보 및 접근(10, 11, 12조).* 데이터 주체는 자신의 개인 데이터가 처리될 때 이 사실을 알 권리가 있다. 처리를 책임지는 당사자(데이터 통제자)는 그 이름과 주소, 처리의 목적, 데이터 수령인 및 처리과정의 공정성 확보에 필요한 모든 기타 정보를 제공해야 한다. 데이터 주체는 자신에 관한 모든 처리 데이터에 접근할 권리와 불완전하거나 부정확하거나 또는 데이터 보호 규정에 따라 처리되지 않은 데이터의 수정, 삭제 또는 차단을 요구할 권리가 있다. (12조).

2. *법적 기초(7조).* 데이터 처리는 항상 6개의 법적 기초 중 하나에 근거해야 한다. 데이터는 다음의 경우 처리될 수 있다.

   - 동의를 득한 경우,
   - 계약 이행이나 계약 체결에 처리가 필요한 경우
   - 법적 의무 이행에 처리가 필요한 경우
   - 데이터 주체의 중요한 이해관계 보호에 처리가 필요한
   - 공공의 이익을 위한 과제 수행이나 공공 권한 행상에 처리가 필요한 경우

1) 1995년 10월 24일자 개인 데이터 처리 및 그러한 데이터의 자유로운 이동과 관련해 개인의 보호에 관한 유럽의회 및 유럽 이사회 시행령 95/46/EC

- 데이터 통제자나 제 3자가 추구하는 입법적 이해관계를 위해 처리가 필요한 경우. 단, 데이터 주체의 기본권리와 자유라는 이해관계가 그러한 이해관계에 우선되는 경우는 제외.

3. *입법적 목적 (6.b조).* 개인 데이터는 구체적인 명시적 입법 목적을 위해서만 처리될 수 있고, 그러한 목적에 부합하지 않는 방식으로 추가 처리되어서는 안 된다.

4. *비례 원칙(6조).* 개인 데이터는 데이터가 수집된 목적과 관련해 적절하고 관련이 있으며 과도하지 않는 경우에만 처리되거나 추가 처리될 수 있다. 따라서 데이터는 정확해야 하며, 최신의 것이어야 하고, 필요한 기간 이상 데이터 주체의 식별이 가능한 형태로 유지되어서는 안 된다.

5. *민감한 데이터(8조).* 종교적 신념, 정치적 견해, 성적 성향, 인종, 무역협회 회원 등과 같은 민감한 개인 데이터를 처리할 경우에는 좀 더 엄격한 규정을 적용해야 한다.
6. *반대할 권리(14조).* 데이터 주체는 언제라도 다이렉트 마케팅 용도로 개인 데이터를 처리하는 것에 반대할 수 있다.

7. *자동 의사 결정(15조).* 법적 효력이 발생하거나 데이터 주체에 중대한 영향을 미치는 결정은 자동 데이터 처리과정에만 의존해 이루어져서는 안 된다. 자동 의사 결정 과정을 사용할 경우에는 이의제기의 형태를 제시해 주어야 한다.

II. 새로운 입법 필요성: 유럽에서 부족한 것이 무엇인가?

1. 기술적 변경사항

유럽집행위원회가 제안한 변경내용은 기술적 변화에 크게 영향을 받고 있다. 전자 처리, 온라인 서비스의 성장 및 개인 데이터의 양이 계속해서 증가한다는 사실 등은 수많은 법규의 변경 제안을 자극했다. 유럽집행위원회는 온라인 환경에서 개인 데이터를 더 잘 보호하고 시민들에게 자신의 데이터에 관해 더 많은 통제력을 지닐 수 있게 해주려 하고 있다.

2. 유럽의 경제 성장

유럽집행위원회는 기업들이 유럽에서 더 쉽게 사업을 할 수 있게 하기 위해 민간 분야에 관한 법규들을 간소화하고자 하고 있다. 27개의 서로 다른 데이터 보호법을 하나의 규정으로 대체함으로써 사업체가 이를 준수하는 것이 더 쉬워질 것이다. 또한 처리 조작을 데이터 보호청(이하 DPA로 지칭)에 통지해야 하는 것과 같은 행정적 요구사항도 없어지게 될 것이다.

3. 집행 및 제재

유럽에서의 데이터 보호법 집행이 일관적으로 강력하게 시행된 적이 한 번도 없다. 일부 데이터 보호청은 상대적으로 강력한 반면, 다른 보호청은 직원 수가 심각하게 부족한 실정이다. 직원 수가 부족한 DPA는 데이터 보호법을 적절하게 집행할 수 없다. 집행과 관련된 또 다른 이슈는 일부 회원국에서는 최대 제재 한도가 매우 낮은 수준에 머물고 있다는 점이다. 예를 들어, 네덜란드의 경우 데이터 보호와 관련된 특정 행정적 요구사항을 위반한 것에 대한 최대 제재 조치는 EUR 4,500(650만원)에 불과하다. DPA는 데이터 보호법을 위반한 혐의가 있는 회사나 정부 조직을 수사할 수 있는 권한이 없다. 그러한 위반 행위가 성립되었을 때 DPA는 위반 사항에 관한 시정이 이루어지지 않은 기간 동안 높은 벌칙을 부과할 수는 있다. 하지만 그러한 제도는 DPA가 연간 많은 사례들을 수사할 수 있는 충분한 시간이 있는 경우에만 성공적일 수 있다.

4. 개방 규범

마지막으로 위에서 언급한 데이터 보호 원칙인 주로 개방형 규범이다. 이는 이 원칙들이 탄력성을 지닐 수 있게 해주며, 민간 분야와 공공 분야를 아울러 여러 상황에 적용될 수 있게 해준다. 다른 한편, 개방성은 애매함과 불확실성을 가져올 수도 있다. 또한 만은 용어들이 회원국 간에 서로 다른 의미로 해석될 수도 있다. 유럽 입법자들은 그러한 개방형 규범들을 판례법으로 보완해야 한다고 믿고 있다. 하지만 데이터 보호와 관련된 문제에 관한 법원 판례가 그리 많지 않다. 프라이버시와 데이터 보호와 관련된 법원 판례는 보통 유럽 인권헌장 7조와 8조, 그리고 유럽 인권협약 8조에 기초해 다루어지고 있다. 이러한 조항들은 개인의 사적인 생활과 개인 데이터의 보호권리를 보호해주고 있다. 대부분 데이터 보호 요구상황에 직면한 기업들은 정확하게 어떤 개방형 규범(예를 들면 '적절성')이나 입법 상의 이해관계에 따라야 하는지를 파악하는데 어려움을 겪고 있다. 유럽집행위원회는 법적 개념을 보다 분명하게 해서 현행 법규에 세부적인 내용을 채우고자 하고 있다.

III. 규정 안이 제안하는 변경사항

유럽집행위원회는 2012년 1월 새로운 데이터 보호 규칙안[2]을 제시했다. 첫째, 유럽집행위원회는 법적 구조를 시행령(directive)의 형태에서 규정(regulation)으로 바꾸고자 하고 있다. 규정은 유럽 회원국가 내에 직접 적용되며 집행될 수 있을 것인데, 이것이 의미하는 바는 유럽 전역에 걸쳐 동일한 법이 될 것이라는 점이다. 이는 사업체에게는 이득이 되는 것이라 할 수 있는데, 그 이유는 사업체들이 더 이상 서로 다른 수많은 규칙을 준수해야 할 필요가 없어지기 때문이다.

둘째, 유럽집행위원회는 기존의 제도에 관한 흥미로운 업데이트를 제안하였다. 이러한 업데이트 사항들은 데이터 통제자(개인 데이터를 처리하는 기업 및 정부 조직)들에 대한 행정적 제재의 수를 줄이고 데이터 주체(자신의 데이터가 처리되는 시민들)에 대해서는 더 많은 통제력과 투명성을 제공해주기 위한 것이다.

시민들을 위한 내용은 무엇인가?

이제 시민들에게 시민들의 개인 데이터를 더 잘 보호할 수 있게 하기 위한 규정안에 담겨 있는 가장 흥미로운 신규 조항들을 개략적으로 살펴볼 것이다.

보호 데이터에 대한 더 나은 정의(규정안 4(1)조)

유럽집행위원회는 장치 번호, IP 주소, 쿠키 식별자(identifier) 등과 같은 온라인 식별자는 자연인을 식별할 수 있다는 사실을 분명하게 밝힘으로써 '개인 데이터'의 정의를 약간 변경시킬 것을 제안하고 있다. 이렇듯 그러한 식별자 데이터는 규정안의 범위에 포함되며, 보호될 수 있다

보다 엄격한 동의에 관한 규칙(규정안 7조)

유럽집행위원회는 동의에 관한 요건을 일반적인 동의에서 '명시적 동의'로 변경할 것을 제안하고 있다. 이는 데이터 통제자가 시민에게서 동의를 얻고자 할 때 통제자가 명시적으로 해당 인이 특정 용도에 자신의 개인 데이터를 사용하는 것에 동의하는지를 물어야 한다는 것을 의미한다. 이는 구체적으로 시민들에게 자신의 데이터에 대해 더 많은 통제력을 부여하고 동의가 일반 조건에 감추어져 있는 상황을 방지하기 위한 것이다.

둘째, 이는 동의를 구하는 데이터 통제자와 데이터 주체(시민)간 유의미한 불균형이 존재하는 경우에는 동의를 타당하게 구한 것으로 간주할 수 없다는 것을 의미한다. 따라서 의사의 경우 개인 데이터의 처리를 동의에만 기초해 진행할 수 없고, 고용주도 마찬가지다. 이들은 데이터 처리를 위해 또 다른 법적 근거를 마련할 필요가 있다.

---

2) 2012년 1월 25일자 개인 데이터 처리 및 그러한 데이터의 자유로운 이동과 관련해 개인의 보호에 관한 유럽의회 및 유럽 이사회 규정 제안 (일반 데이터 보호 규정), (COD) 2012/0011

잊혀질 권리(규정한 17조)

규정안에 있어 가장 논쟁이 되고 있는 추가 사항 중의 하나는 소위 “잊혀질 권리“에 관한 논쟁이다. 이는 처음에는 논쟁을 유발하는 제목 때문에 시작된 것이었다. 주장하는 바와는 달리, 잊혀질 권리는 시민들이 자신의 데이터를 모든 환경에서 삭제할 권리가 있다는 것을 의미하지는 않는다. 하지만 이 조항은 초안 작성이 제대로 되어 있지 않아 이해하기가 힘들다. 이 조항은 이 조항의 정확한 적용범위에 관해 심각한 우려를 자아내었으며, 언론의 자유를 침해할 수 있는 가능성에 관한 논쟁을 불러일으키기도 하였다.

유럽집행위원회는 모든 시민들이 데이터 통제자에게서 자신의 개인 데이터의 추가 확산을 금지할 권리를 얻을 수 있다고 제안하였다. 또한, 데이터 통제자가 개인 데이터를 공개할 경우, 데이터 통제자는 이 데이터를 처리하는 제 3자에게 시민이 정보 삭제와 개인 데이터 사본 정보와의 링크를 삭제해줄 것을 요청했다는 사실을 알리기 위해 필요한 모든 합리적 조치를 취해야 한다.

이 권리에 대한 여러 예외 조항이 있는데, 예를 들면, 언론의 자유를 행사, 공공보건 상의 이유, 또는 통계적, 역사적, 과학적 연구 목적으로 데이터를 보유하는 것이 필요한 경우 등과 같은 경우가 그것이다. 그럼에도 불구하고 유럽집행위원회가 제안한 형태의 잊혀질 권리는 데이터 통제자에게 자신이 발행한 데이터를 삭제하는 것뿐 아니라 제3자도 데이터를 삭제해야 하는 등 너무 많은 부담을 줄 수 있다는 우려가 제기되고 있다.

자신의 데이터를 가질 수 있는 권리(데이터 이식성(portability), 규정안 18조)

유럽 집행 위원회는 개인 데이터의 접근, 삭제, 수정 권리에 추가 사항을 도입했다. 규정안에 따르면 데이터 주체는 원하는 경우 한 데이터 통제자로부터 다른 통제자에게 데이터를 이식할 수 있게 자신의 개인 데이터에 대한 전자 사본을 얻을 수 있게 되어 있다. 이 새로운 조항은 소셜네트워크의 경우 고객의 록 인(lock-in)을 방지하기 위한 목적이다. 하지만 이는 예를 들어 자신의 텔레콤 데이터를 다른 사업체에 전달하고 정확한 용도에 기초해 더 좋은 새로운 제안을 받거나 분석할 수 있는 개요 데이터를 취득해 가정에서의 에너지 소비를 추적할 수 있게 해주는 등의 다른 용도로도 사용할 수 있다. 단순한 사본을 넘어선 이점은 디지털 파일이어서 스스로 데이터를 분석하거나 자신이 선택한 다른 회사에 이 데이터를 업로드할 수 있다는 점이다. 록 인을 방지하는 것 외에 이 조항은 시민들이 한 회사에 만족하지 못하는 경우 다른 회사로 이동하는 것을 더 용이해지게 함으로써 유럽 내 서비스 경쟁을 촉진시키기 위한 목적을 지니고 있다.

프로파일링을 금지한 새로운 규칙(규정안 20조)

현 시행령의 15조는 여러 기준을 충족하는 경우가 아니면 자동 의사 결정을 금지하고 있다. 예를 들어 자동화된 결정은 민감한 데이터에만 기초해 이루어질 수 없다. 자동화된 의사 결정(프로파일링)이 발생했다는 사실과 그러한 프로파일링의 결

과에 관한 정보 등과 같이 추가적인 안전장치가 있어야 한다.

데이터 위반은 DPA와 시민에게 보고해야 한다(규정안 31조 및 32조)

규정안에는 데이터 통제자가 데이터 위반 사항을 DPA에 가능한 빨리(일반적으로 24시간 이내) DPA에 보고할 것을 요구하고 있다. 위반 사항이 시민에게 부정적 영향을 미칠 경우, 위반 내용을 시민에게도 보고해야 한다.

새로운 준수 제도 및 강화된 벌칙(규정안 79조)

새 규정안에 따르면, 유럽 국가들의 데이터 보호청들은 서로 다른 보호청 간의 차이를 극복하기 위해 밀접하게 협력하게 될 서이다. EU 전체에 걸쳐 일관성 있는 집행을 위해 한 보호청에서 내린 결정을 다른 보호청에 제출하게 될 것이다.

둘째 모든 DPA에게는 강력한 제재 가능성을 포함해 동일한 집행 권한이 부여된다. 데이터 보호 규정 위반은 해당 회사의 전 세계 매출액의 0.5%~최대 2%까지를 벌침금으로 부과할 수 있게 된다.

IV. 정치 활동 현황

규정안을 유럽집행위원회가 제출한 이후, 유럽 이사회(장관 이사회, 각 회원국의 사법부 장관으로 구성)와 유럽 의회(EP)는 규정안에 코멘트를 제시하고 이에 수정을 가했다. 이사회 내의 협의안은 비밀이며, 협상 회의의 결과만 발표되고 있다. 유럽의회의 결정은 좀 더 공개적이다. 따라서 이 법안에 영향을 행사하고 유럽의회 회원들이 규정안에 수정을 가하게 설득할 로비스트들의 대상은 의회가 되고 있다.

1. 브뤼셀 로비

이 규정안에 대한 로비스트들의 영향력은 매우 강력한 것으로 입증되고 있다. 담당 위원장인 Ms. Vivian Reding은 데이터 보호법을 둘러싼 로비는 '그 어떤 로비보다도 극심하다'고 말하고 있다.[3)]

미국과 유럽의 인터넷 및 IT 기업들은 통신사, 은행, (온라인) 광고업체, 출판사 및 보험사와 마찬가지로 로비에 열심이다. 이러한 로비의 결과 1년이 조금 넘는 기간 동안 놀라운 숫자인 총 4,000개의 수정 사항이 제시되었다. 호주 활동가의 연구결과에 따르면[4)], 많은 유럽의회 회원들이 사업체 로비 브리핑에서 제안내용을 그대로 복사해오고 있는 것으로 나타났다. 특히 보수적인 유럽국민당(European People's

3) http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html
4) 모든 수정 사항의 개요 및 정치가들이 가장 많이 복사한 내용은 www.lobbyplag.eu 참고

Party: EPP) 소속의 정치인들은 자신의 수정사항을 제시하기 위해 이러한 방법을 사용하고 있다. 대부분의 수정안들은 데이터 처리와 관련해 더 많은 융통성과 시민들의 개인 데이터를 보관, 분석, 사용 및 조합하는데 있어 더 많은 자유를 기업체에 부여하고자 하고 있다.

유럽의 디지털 시민 권리 활동가들 또한 유럽 의회를 대상으로 로비를 벌이고 있지만, 대부분 그 수가 부족한 실정이다.

2. 유럽의회 투표 결과

유럽의회는 아직 이 문제에 대해 총회 투표를 실시하지는 않았지만, 의회 내 위원회에서는[5] 3차례의 투표가 진행되었었다. 이 의견 투표의 결과는 총회 투표 결과를 예측해볼 수 있는 좋은 지표가 된다. 의견 투표 결과는 모든 위원들이 시민의 권리 보다는 사업체의 이해를 더 선호한다는 사실을 보여주고 있다. 이는 유럽집행위원회가 새로 제시한 많은 안들에 변화를 가져왔다. 더 이상 동의를 명시적으로 받을 필요가 없어졌고, 데이터 이식성은 제약을 받으며, 데이터 위반 통지도 심각한 경우에만 필요하고, 프로파일링에 관한 규정도 더 관대해졌다. 제재 조치는 삭감되었고, 유럽의회 회원들은 보호를 덜 필요로 하는 개인 데이터의 특별 하위 범주(소위 '익명 데이터'는 필명으로 대체되었다)를 도입했다. 많은 유럽의회 회원들은 데이터를 제 3국에 수출하는 것에 관해 이들 국가에서의 개인 데이터 보호 수준과 무관하게 좀 더 탄력적인 규정과 덜 엄격한 용도 제약 원칙을 지지하고 있다.

3. 다음 단계

시민 사회의 관점에서 보면, 지금까지의 투표 결과는 매우 실망스럽다 할 수 있다. 다음 단계는 LIBE(Civil Liberties, Justice and Home Affairs) 위원회 투표로서, 이 위원회는 이 문제에 대해 주도적인 위원회이다. 따라서 LIBE의 회원인 의회 내 책임 의원들은 이전 투표 결과를 고려해 2013년 10월 21일로 예정되어 있는 투표 이전에 규정안 패키지를 제시하게 될 것이다.

이전 결과를 고려할 때, 그러한 패키지에 많은 긍정적 솔루션이 포함될 수는 없다. 하지만 의회뿐 아니라 유럽집행위원회 및 이사회가 총회 투표 회기에서 유럽의회 과반수 이상의 찬성에 의해 승인을 받아야 하는 최종 문구에 합의하기 전 협상 과정에서 동일한 권한을 가지고 있다. 유럽집행위원회가 원안을 극단적으로 완화시킨 법안에 동의할 가능성은 그리 높지 않아 보인다.

---

5) 관련 의견 위원회로는 내수 시장 및 소비자 보호(Internal Market and Consumer Protection: IMCO), 산업, 연구 및 에너지(Industry, Research and Energy : ITRE) 및 법무(and Legal Affairs : JURI) 위원회가 있음.

4. 결론: 시민들에게 무엇이 남았는가?

비록 완전히 실망을 하기에는 아직 이른 감이 없지 않지만, 현재의 시행령에서 누리는 데이터 보호 보다 더 나빠진 데이터 보호법과 프라이버시 보호법으로 결론지어질 가능성도 없지 않다. 유럽집행위원회는 문제들을 들추어내서 데이터 보호법을 근대화하고자 노력해왔지만, 그러한 노력은 현재 정확하게 그 반대 결과를 노리는 반대 제안에 직면해 있다.

이는 모든 사람들이 시민들의 개인 데이터가 매우 소중한 것이며, 우리 경제와 사회에 있어 그 역할이 계속해서 커지고 있다는 사실을 잘 인식하고 있기 때문에 역설적인 상황이라 볼 수 있다. 안타깝게도 정치가들은 개인 데이터를 보호할 가치가 있는 기본적 권리로 인식하지 않고 단순히 디지털 경제의 돈다발로만 여기고 있는 것처럼 보인다.

국문초록

유럽 개인정보보호 개정이 시민에게 미치는 영향 : 어떤 선택을 할 것인가

Janneke Slöetjes

시민들의 개인 데이터와 프라이버시를 보호하는 유럽 법률은 전 세계적으로 최고 수준의 데이터 보호 법률이라는 위치를 차지하고 있다. 2012년 1월 유럽연합집행위원회(EC)는 이러한 법규 개혁을 개시해 데이터 보호 및 프라이버시의 미래에 대한 격렬한 논쟁을 완화시킨 데이터 보호 규정안(Draft Regulation)을 도입했다. 이 안은 새로운 기술을 도입하려 하고 있으며, 시민 개인과 사업체 둘 모두에 보안 및 선택 기회를 제공하고 있다. 그러나 그것으로 약속한 것을 성취해낼 수 있을까?

유럽집행위원회는 기존 법규에 여러 새로운 개념을 도입했다. 이는 사업비용을 경감하고 시민 개인이 자신의 개인 데이터를 사용하는데 있어 더 많은 통제력을 발휘할 수 있게 하기 위한 것이었다. 변경 내용으로는 온라인 환경에서 데이터를 더 잘 보호하기 위한 목적의 개인 데이터를 더 잘 정의하는 것, 동의를 얻는 것에 관한 좀 더 엄격한 규정과 소위 망각할 권리 등이 포함되어 있는데, 이러한 변경내용은 시민들로 하여금 자신에 관해 공개된 정보를 삭제할 수 있게 해준다. 이러한 새로운 권리는 언론의 자유를 보호하는 것에 관해 의문을 제기하고 있다. 뿐만 아니라 제안내용에는 시민들이 자신의 데이터 전체 사본을 얻을 수 있는 권리와 데이터 침해 통지 규정과 데이터 보호 법률을 위반한 기업이나 정부에 대해 더 높은 수준의 제재 조치 등이 포함되어 있다.

유럽 의회는 이 입법안에 대해 수많은 반대 제안에 직면해오고 있다. 이러한 제안들 중 대부분은 사업체가 자신들의 이익을 위해 시민 데이터를 처리할 수 있는 여지를 더 많이 제공하기 위한 목적을 지니고 있기 때문에 프라이버시 보호를 축소시키는 결과를 낳게 될 것이다. 이는 의회 의원들이 도입한 상당수의 제안과 수정안이 로비스트들의 제안에서 비롯된 것이기 때문에 그리 놀랄 일도 아니다.

따라서 이 입법 과정이 어떻게 결말을 맺을지는 매우 불확실하다. 유럽인들은 현재 수준 보다 자신들의 개인 데이터 보호 수준이 축소되는 것으로 결말을 맺을 수도 있다.

본 논문은 데이터 보호법의 업데이트 필요성을 분석하고, 유럽집행위원회가 제안한 새로운 추가 사항을 탐색해볼 것이다. 마지막으로 본 논문은 정치적 활동 상태와 가능한 결과에 대한 설명을 제시할 것이다.