한국법제연구원–경북대학교 공동학술대회
International Conference

정보화시대에 따른 개인식별번호법제의 쟁점과 과제

The comparative legal issues
regarding Individual Identifiable Numbering System
among 4 Countries in the Pacific Rim in the information age

일 시 | 2016년 6월 10일 금요일 13:00–18:00

장 소 | 경북대학교 법학전문대학원 서관 507호

주 최 | 한국법제연구원, 경북대 법학연구원

주 관 | 한국법제연구원 비교법제연구실,
경북대 법학연구원 지방자치·환경및계획법연구센터

KLRI KOREA LEGISLATION RESEARCH INSTITUTE

KNU KYUNGPOOK NATIONAL UNIVERSITY

프로그램

전체사회: **이상윤** | 한국법제연구원 연구위원

13:00~13:20	등록
개회사	**김창록**	경북대학교 법학연구원 원장
환영사	**이 원**	한국법제연구원 원장
축 사	**권오걸**	경북대학교 법전원 원장
13:20-13:30	기념촬영

제1세션 한국과 일본의 개인식별번호법제의 현황과 문제점

사 회	**신봉기**	경북대학교 법전원 교수
13:30-14:20	**제1주제** **한국의 개인식별번호법제 현황과 문제점**
발 표	**강경근**	숭실대학교 교수
토 론	**박광동**	한국법제연구원 연구위원
토 론	**성중탁**	경북대학교 교수
14:20-15:10	**제2주제** **일본의 개인식별번호법제 현황과 문제점**
발 표	趙元済	駒沢大学大学院法曹養成研究科 교수
토 론	**김수홍**	한국법제연구원 부연구위원
토 론	**김민섭**	국가인권위원회 사무관
15:10-15:30	Coffee Break

제2세션 미국과 대만의 개인식별번호법제의 현황과 문제점

사 회	**정하명**	경북대학교 법전원 교수
15:30-16:20	**제3주제** **미국의 개인식별번호법제 현황과 문제점**
발 표	Erin Murphy	영남대학교 법전원 교수
토 론	**최지연**	한국법제연구원 부연구위원
토 론	**김성배**	국민대학교 교수
16:20-17:10	**제4주제** **대만의 개인식별번호법제 현황과 문제점**
발 표	翁淸坤	輔仁大學財經法律學系 교수
토 론	**이상모**	한국법제연구원 부연구위원
토 론	**권세훈**	경성대학교 강의교수
17:10-17:20	Coffee Break

종합토론

사 회	**신봉기**	경북대학교 법전원 교수
17:20-17:50	참가자 전원
17:50	폐회식

SESSION 1

SESSION 2

PROGRAM

Moderator : **LEE, Sang-Yoon** | Director , KLRI

13:00~13:20	**Registration**
Opening Remarks	**KIM, Chang ROK** | Director, KNU Law Research Institute
Welcome Address	**LEE, Won** | President, Korea Legislation Research Institute
Congratulatory Speech	**KWON, Oh Geol** | Dean, KNU LAW School
13:20-13:30	**Group Photo**

SESSION 1

Session Ⅰ	**Legal issues regarding Korean and Japanese Individual Identifiable Numbering System**
Moderator	**SHIN, Bong-Ki** | Professor, KNU Law School
13:30-14:20	**Legal issues regarding Korean Individual Identifiable Numbering System (Residence Register Number)**
Presenter	**KANG, Kyung-Keun** | Professor, Soongsil University
Discussant	**PARK, Kwang Dong** | Senior Research Fellow, KLRI
Discussant	**SUNG, Joong Tak** | Professor, KNU Law School
14:20-15:10	**Legal issues regarding Japanese Individual Identifiable Numbering System**
Presenter	**CHO, WonJae** | Komazawa University, Japan
Discussant	**KIM, Suhong** | Research Fellow,KLRI
Discussant	**KIM, Min Seop** | Administrative Official, National Human Rights Commission of Korea

15:10-15:30	**Coffee Break**

SESSION 2

Session Ⅱ	**Legal issues regarding American and Taiwanese Individual Identifiable Numbering System**
Moderator	**SHIN, Bong-Ki** | Professor, KNU Law School
15:30-16:20	**Legal issues regarding American Individual Identifiable Numbering System**
Presenter	**Erin MURPHY** | Professor, Yeungnam University Law School
Discussant	**CHOI, Ji Yeon** | Research Fellow, KLRI
Discussant	**KIM, Sung Bae** | Professor, Kookmin University
16:20-17:10	**Legal issues regarding Taiwanese Individual Identifiable Numbering System**
Presenter	**C.K.** | Professor, Fu Jen Catholic University(Taiwan)
Discussant	**LEE, Sang Mo** | Research Fellow, KLRI
Discussant	**KWON, Sea Hoon** | Porfessor, Kyungsung University

17:10-17:20	**Coffee Break**

	Comprehensive discussion
Moderator	**SHIN, Bong-Ki** | Professor, KNU Law School
17:20-17:50	**Attendees**

17:50	**Closing**

정보화시대에 따른 개인식별번호법제의 쟁점과 과제

The comparative legal issues regarding Individual Identifiable Numbering System among 4 Countries in the Pacific Rim in the information age

CONTENTS

개회사

여러분 안녕하십니까?

오늘 경북대학교 법학연구원이 한국법제연구원과 함께 “정보화시대에 따른 개인식별번호법제의 쟁점과 과제”를 주제로 국제학술대회를 개최하게 된 것을 매우 기쁘게 생각합니다.

지금 전 세계는 과거 그 어느 시대에도 경험하지 못했던 정보화시대라는 신천지 속에서 살아가고 있습니다. 정보화시대는 인류에게 은총인 동시에 도전이기도 합니다. 과거와는 비교가 되지 않는 신속함과 다양성을 가져다주는 한편으로, 새로운 권리 침해의 위험 또한 만들어내고 있습니다. 특히 정보화시대를 맞아 개인정보 보호의 필요성은 날로 커지고 있습니다. 세계 각국에서 개인식별에 관한 법제가 주목받고 있는 것은 바로 그 때문일 것입니다.

그 점에서 오늘의 학술대회는 참으로 중요한 주제를 다루는 의미 깊은 자리라고 생각합니다. 특히 환태평양 4개국, 즉 한국, 미국, 일본, 대만의 우수한 학자들을 발표자와 토론자로 모시고, 네 나라의 개인식별번호법제를 비교·검토하는 자리라는 점에서 각별한 의의를 가진다고 생각합니다.

오늘의 학술대회가 정보화시대의 중요 현안인 개인식별번호법제에 대해 상호 비교하면서 새로운 가능성을 모색하는 소중한 자리가 되리라고 믿습니다. 또한 환태평양 4개국 사이의 우호증진을 위해서도 좋은 계기가 되리라고 믿습니다.

오늘의 이 훌륭한 학술대회를 공동으로 주최해주신 한국법제연구원의 이원 원장님을 비롯한 여러분, 멀리서 경북대학교를 찾아주신 발표자와 토론자 여러분께 다시 한 번 깊이 감사를 드립니다. 오늘의 국제학술대회가 커다란 성공을 거두게 되기를, 그리고 여러분 모두 항상 건강하시고 건승하시기를 기원합니다.

감사합니다.

2016. 6. 10.

경북대학교 법학연구원 원장 **김창록**

환영사

존경하는 내외 귀빈 여러분! 저는 경북대학교 법학연구원과 함께 이번 공동학술대회를 주최하는 한국법제연구원 원장 이원입니다.

먼저 영남지방을 대표하는 명문인 경북대학교 법학연구원과"정보화시대에 따른 개인식별 번호법제의 쟁점과 과제"라는 주제로 공동학술대회를 개최하게 된 것을 매우 뜻깊고 기쁘게 생각합니다. 공동학술대회의 기회를 마련해주신 김창록 법학연구원장님, 바쁘신 중에서도 축사를 해 주시는 경북대학교 법학전문대학원의 권오걸 원장님과 사회자, 발표자, 토론자 그리고 자리를 함께 해주신 모든 분들께 감사의 말씀을 드립니다.

주지하는 바와 같이, 우리나라에서는 지난 2014년 주요 카드사에서 보유하고 있던 1억 400만여 건의 개인정보가 유출되는 사건이 발생하였습니다. 그리고 미국에서도 지난 2015년 수많은 건강보험업체들이 관리하고 있던 고객 데이터베이스를 공격당해 고객 정보들이 유출되는 사건이 발생하였습니다. 이와 같은 사태에 직면한 세계 각국은 개인정보 침해사고를 최소화하기 위해 개인식별정보의 수집·관리를 엄격히 제한하는 등 개인정보에 대한 보호대책을 마련하고 있습니다. 우리나라에서도 최근 해킹이나 개인정보 유출로 인해 생명·신체·재산상의 피해를 입거나 입을 우려가 있는 경우 주민등록번호를 변경할 수 있도록 주민등록법을 개정하였고, 또 개인정보보호법을 개정해서 개인정보 처리자의 개인정보 분실·유실 등으로 인해 발생한 손해에 대한 징벌적 배상제도와 법정손해배상제를 도입하는 등 개인정보 보호 및 관리를 대폭 강화하고 있습니다.

이처럼 개인정보의 보호를 위한 일련의 대응책을 마련하고 있는 우리나라의 입장에서는, 서로 다른 개인식별 번호법제를 운영하고 있는 우리나라와 미국, 일본, 대만 등 환태평양 4개국의 개인식별번호 법제를 상호 비교·분석함으로써, 정보화시대에 보다 적합한 개인식별번호 법제를 구축해 나가는 데에 소중한 정보와 의미 있는 시사점을 얻을 수 있을 것으로 생각합니다.

우리 연구원은 국내 유일의 법제전문 국책연구기관으로서 정책현안에 대한 입법적 대안을 제시하고, 국내외 법제를 조사·연구하고 법령정보를 체계적으로 수집·관리함으로써 국가입법정책의 지원과 법률문화의 향상에 기여하는 것을 설립목적으로 하고 있습니다. 오늘 이 자리에 모이신 환태평양 4개국의 개인식별정보 전문 연구자 분들이 제시해 주시는 각국의 경험과 노하우는 우리 연구원에게도 많은 도움이 될 것으로 기대합니다.

끝으로 오늘 공동학술회의를 위해 많은 수고를 해주신 경북대학교 법학연구원과 한국법제연구원 관계관 여러분들께 진심으로 감사드립니다.

2016. 6. 10.

한국법제연구원장 **이 원**

축사

여러분 안녕하십니까? 지난 2016년 6월 7일부터 경북대학교 법학전문대학원 원장을 맡게된 권오걸 교수입니다. 제가 원장을 맡고 나서 처음으로 개최되는 국제학술대회에 축사를 하게 되어 영광입니다. 앞에서 김창록 경북대학교 법학연구원 원장님, 이원 한국법제연구원 원장님께서 말씀하신 바와 같이 정보화 시대에서의 개인식별번호의 보호 필요성은 너무나도 명백하다고 할 것입니다. 이러한 시대적 요구에 부응하여 오늘 경북대학교 법학연구원과 한국 법제연구원과 공동으로 "정보화시대에 따른 개인식별번호법제의 쟁점과 과제"라는 제목으로 환태평양 4개국 즉 우리나라, 미국, 일본, 대만 등에서 오신 우수한 학자들을 모시고 각국의 개인식별번호 법제를 비교하고 논의할 수 있는 국제학술대회를 가지게 된 것을 진심으로 축하드립니다. 특히 먼 길을 와주신 대만의 翁清坤 교수님, 일본의 趙元済 교수님, 강경근 교수님, Erin Murphy 교수님 등 발제자 여러분께 감사를 드립니다. 제가 저희 법학전문대학원에서 지리적으로 가장 먼 곳에서 오신 분들부터 먼저 소개 말씀을 드렸습니다. 토론자와 사회자 여러분에게도 감사의 말씀을 드립니다. 또한 저희 경북대학교 법전원과 인연을 잊지 않으시고 다시 찾아주신 이원 한국 법제연구원 원장님과 여러분께도 감사의 말씀을 드립니다. 학내 김창록 법학연구원 원장님과 신봉기 법학연구원 지방자치·환경및계획법연구센터장에게도 감사의 말씀을 드립니다. 아무쪼록 오늘 저희 법학전문대학원에서 좋은 학술논의의 장이 가지시고 환태평양 4국의 개인식별번호법제에 대한 이해의 증진은 물론 상호 친선의 계기도 되시기를 기원합니다. 대구는 여러분 잘 아시는 바와 같이 우리나라에서 가장 더운 도시로 유명합니다. 날씨가 최근 갑자기 더워져서 여름이 성큼 다가온 것 같습니다. 저희 법학전문대학원과 대구에 계시는 동안 더욱 건강에 유의하시고 즐거운 시간 가지십시오. 한국 법제연구원-경북대학교 공동 국제학술대회의 성공을 기원하면서 다시금 축하드립니다. 감사합니다.

2016. 6. 10.

경북대학교 법학전문대학원장 **권오걸**

Session 1

한국과 일본의 개인식별번호법제의 현황과 문제점

Session 1-1

한국의 개인식별번호법제 현황과 문제점

강경근 | 숭실대학교 교수

한국의 개인식별번호법제 현황과 문제점

Ⅰ. 주민등록번호법제 현황

1. 주민등록번호의 개념·연원·역기능

(1) 주민등록번호 개념과 부여 체계

한국에서 개인식별번호법제로 인정되고 있는 대표적 규범은 '주민등록번호'에 관한 「주민등록법」이다. 이 법은 주민번호라는 개인식별번호를 창출하는 법이면서 동시에 그 보호 법제로 기능한다. 주민등록번호는 1968년 도입 후 1975년에 이르러 지금과 같이 개인을 명확히 손쉽게 식별하는 기능을 갖게 된다. 이런 개인식별번호의 기능은 주민등록번호 자체의 일신전속성, 고유성, 불변성 등의 특징에 의하여서이다. 이후 1990년대 정보화의 진전으로 주민등록번호는 온라인 개인식별 및 인증수단으로 폭넓게 사용되었다.[1] 이런 인식을 기초로 하면서, 본고에서는 개인식별번호법제로 대표되는 주민등록번호법제인 '주민등록법'을 중심으로[2], 그 현황과 문제점 등을 최근 헌법재판소 결정 등을 소재로 논의하는 것으로 한다.

「주민등록법」에 의거하는 주민등록번호는 시장·군수 또는 구청장이 주민에게 부여하는 '개인별로 고유한 등록번호'로서(제7조 제3항), 「가족관계의 등록 등에 관한 법률」에 따른 출생신고와 더불어 주민등록번호가 같이 부여되고 있다. 시장·군수 또는 구청장은 주민등록사항을 기록하기 위하여 전산정보처리조직으로 개인별 및 세대별 주민등록표와 세대별 주민등록표 색인부를 작성하고 기록·관리·보존하여야 한다(동조 제1항). 이 주민등록번호는 주민등록표의 필수적 기재사항으로[3], 주민등록표 정리의 기준이 되는 정보이다. 주민등록표 정리는 '주민등록번호

---

1) 강경근, 주민등록과 전산화 그리고 프라이버시, 「아·태공법연구」(제4집 1997); 고문현 外, 『국가신분확인체계 발전방안 연구』(행정안전부 연구용역보고서 2010); 김민섭, 「개인정보의 보호와 활용의 조화에 관한 법제적 연구」(숭실대학교대학원 박사학위논문 2014); 김민호 外, 『주민등록번호제도 개선방안 연구』(국가경쟁력강화위원회 연구용역보고서 2009); 국가인권위원회, 『주민등록번호 사용현황 실태조사』2005; 김영미, 해방 이후 주민등록제도의 변천과 그 성격 -한국 주민등록증의 역사적 연원-, 「한국사연구」(제136호 2007.3); 헌법재판소 헌법재판연구원, 『주민등록번호제에 대한 헌법적 쟁점』2013. 기타 김민섭 박사의 자료와 조언을 참고하였다.

2) 김민섭의 박사논문에서는, "「개인정보보호법」 시행 3년이 경과한 시점에서 주민등록번호 아닌 '고유식별정보' 자체에 대해서는 유의미한 연구를 찾기 어렵다. 따라서 주민등록번호 외 운전면허번호, 여권번호, 외국인등록번호에 굳이 '고유식별정보'라는 별도의 정보 분류를 만들어 엄격처리기준을 적용할 필요가 있는지, 그 규제로 얻어지는 법적·사회적 편익은 무엇인지를 재검토할 필요성이 있다"라고 한다.

3) 주민등록법 시행령 제6조 제1항 및 동 시행령 별지 제1호 서식, 별지 제2호 서식 참조.

순'으로 하여야 하며 구체적으로 개인별 주민등록표는 개인의 주민등록번호 순으로, 세대별 주민등록표는 세대주의 주민등록번호 순으로 각각 정리한다(제9조). 시장·군수 또는 구청장은 관할 구역에 주민등록이 된 자 중 17세 이상인 자에 대하여 주민등록증을 발급하여야 한다(제24조 제1항). 주민등록번호는 주민등록증의 필수적 수록사항이다.[4)]

「주민등록법」 및 동법 시행규칙에는 주민등록번호 구성 체계에 관한 직접적 규정은 존재하지 않는다. 「주민등록법」 시행규칙에서는 "「주민등록법」 제7조 제3항에 따른 주민등록번호는 생년월일·성별·지역 등을 표시할 수 있는 13자리의 숫자로 작성한다"[5)] 만을 정하고 있다. 주민등록번호는 주민등록대상인 주민에 대하여 출생, 귀화 등 새로 발급할 필요성이 있을 때 신고와 더불어 발급된다. 주민등록번호는 앞 6자리와 뒤 7자리로 구성되고, 앞자리와 뒷자리는 "-"로 연결된다. 앞의 여섯 자리 숫자는 생년월일, 뒷 일곱 자리 숫자는 성별과 출생연대, 지역번호, 신고순위, 그리고 오류검증번호(check digit)로 이루어져 있다.[6)]

(2) 주민등록번호의 도입배경과 연원

주민등록제도, 주민등록번호 등의 연혁을 본다. 이들 제도는 일제강점기 1909년 일본「호적법」 및 1922년 「조선호적령」에 따른 호적제도, 1942년 「조선기류령」 및 「조선기류수속규칙」 등에 연원을 둔다. 광복 이후 1947년 거주등록 및 등록표 발급 제도, 1948년 대한민국 정부 수립 후에는 「조선기류령」이 거주자 등록에 관한 제도로 시행되고[7)], 1949년경 양민증, 시·도민증 발급 이후, 1950년 6·25동란전쟁으로 전국에 확대 시행되면서 휴전 후 시·도 규칙 제정 등으로 제도화되었다. 시·도민증 제도는 (국가재건최고회의 1962.1.15. 「기류법」 제정·시행·폐지후) 1962.5.10. 「주민등록법」(법률 제1067호) 제정·시행(6.20.) 등에 의하여 각 시·도 규칙에 따라 운영되다가 1962년 「주민등록법」 제정을 통하여 국가적 신분증 제도로 운영되기 시작하였다. 이후 이 주민등록법은 총 25차례 개정(타법개정 포함)을 거쳐 지금에 이른다.

우리의 주민 거주관계 등록 관련 법제는 주민등록번호와 같은 당사자 확인 기능을 지닌 국가적 신분 증명의 제도로 인하여 국민의 기본권 행사조건을 마련하는 계기가 되었고(예컨대 선

4) 주민등록증의 필수적 수록사항은 성명, 사진, 주민등록번호, 주소, 지문(指紋), 발행일, 주민등록기관이다. 선택적 수록사항으로서 혈액형은 주민의 신청이 있으면 추가로 수록할 수 있다. 재외국민에게 발급하는 주민등록증에는 재외국민임을 추가로 표시하여야 한다. 주민등록법 제24조 제2항 및 제3항.

5) 주민등록법 시행규칙 제2조.

6) 중앙일보, 2011.4.26, '개원 40주년 맞은 KDI', 주민등록번호 부여 체계는 1975년 당시 한국개발연구원(KDI) 연구진이 통계학 지식을 활용하고 미국 사회보장번호(Social Security Number) 시스템을 참고해 만들었다 한다. 주민등록번호 부여 방식은 지역별 총 1억 명까지 주민등록번호를 부여할 수 있고 통일 후에도 우리나라 인구가 1억 명을 넘을 가능성은 없으므로 영구적으로 주민등록번호를 부여해 나갈 수 있다고 밝히고 있다.

7) 행정자치부,『2016 주민등록 인감 법령집』, 3면.

거권이나 교육을 받을 권리 등) 또한 헌법상 기본의무의 이행을 가능케 하며(예컨대 납세, 병역, 교육 등의 의무 등) 나아가 사회복지국가, 정보국가 등 우리 헌법의 국가목표를 실현할 수 있게 하는 제도적 기초로서 그 존재 의의를 가져 왔다. 어찌 보면 대한민국의 근대 국민국가적 형성을 가능케 해 온 '고유한 연결자' 기능이라는 규범적 가치를 지녀왔다 하겠다.[8)]

「주민등록법」 제정·시행 초기 주민등록제도 및 주민등록증에 대해서는 관련 근거가 마련되고 있었으나, 주민등록번호에 대해서는 그 근거가 마련되어 있지 않았었다. 주민등록번호가 처음 법령상 근거를 가지게 된 것은 1968.9.16. 개정「주민등록법」시행령(대통령령 제3585호)이다.[9)] 이 방식은 1975.8.26. 개정「주민등록법」시행령과 동년 11.4. 개정 시행규칙에 의해 지금과 같이 생년월일, 성별, 지역 등을 표시하는 13자리 숫자체계로 변동되었지만, 이후 상당기간 주민등록번호 생성·부여에 관한 법률상 근거는 마련되지 않았다. 2001.1.26.「주민등록법」(법률 제6385호) 일부 개정을 통하여 "시장·군수 또는 구청장은 주민에 대하여 개인별로 고유한 등록번호를 부여하여야 한다"(제7조 제3항) 규정함으로써 비로소 주민등록번호의 부여에 관한 직접적 근거가 '법률'에 반영되어 현재에 이르고 있다.

(3) 주민등록번호의 역기능과 헌법재판소 결정

주민등록번호 제도의 역기능은 그것이 유출·도용되기 시작하면 현행 법제에서 그 변경이 가능하지 아니한 관계로 그 사전 방지 내지 사후구제 통로가 마련되어 있지 못하다는 점에 있다. 특히 인터넷 환경에서의 순기능에도 불구하고 개인정보침해 등 정보인권에 대한 역기능이 지속적으로 제기되었다. 이 환경에서 헌법재판소는 주민등록번호 변경 허용 관련, 2015년 12월 23일 2013헌바68, 2014헌마449(병합) 결정을 내렸다. 아래에서는 헌법재판소 결정의 주요 내용과 시사점을 주민등록번호 제도의 법 규정·제도를 검토하면서 관련 헌법적, 국가 제도적 문제점들을 '주민등록번호 도용 등으로 인한 변경 허용 여부'와 연관하여 살펴본다.

2. 주민등록번호의 헌법적 기능

국민의 개인적 정체성을 식별하는 수단으로 개인마다 일련번호를 부여하는 개인식별번호

8) 강경근, 앞의 논문, 45면.

9) 개인별 주민등록번호(주민등록법 제3조 제1항), 1인1번호(제3항) 등에 기초한「주민등록법」시행규칙(내무부령 제32호)은 주민등록번호 작성과 조정에 관한 사항을 정하였는데 구체적으로 보면 주민등록번호는 지역표시번호, 성별표시번호, 개인표시번호를 차례로 배열하여 작성하고, 지역표시번호 다음에 "-" 표시를 하여 성별표시번호 및 개인표시번호와 연결하며(시행규칙 제1조제1항), 성별표시번호는 남자는 "1", 여자는 "2"로 하도록 하였다(제3항). 즉 초기의 주민등록번호는 총 12자리로서, 6자리씩 2부분으로 나뉘어 있었다.

(personal identification number PIN)로서의 주민등록번호는 주민관리용 식별기능, 표준(범용) 식별기능, 인증기능, 연결기능, 묘사기능 등으로 다양하게 기능한다. 특히 생년월일, 성별 등의 내용을 담는 등으로 개인의 특성을 묘사함으로써, 주민등록번호가 개인 식별이나 인증을 넘어 개개인 의사와 무관하게 본인 특성을 공개한다는 점에서, 이 제도의 상수화가 헌법질서 안에서 근거와 정당성을 가질 수 있을 것인지 및 프라이버시 관련 고찰이 요구된다.[10)]

본고는 논의의 전제로 주민등록번호의 제도화는 국가적 신분확인을 가능케 하는 헌법적 기능을 갖는다는 점을 들고 싶다. 예컨대 국가에 귀속됨을 인정하는 국적은 국가에 대한 명시적 가입의사와 동의 없이도 그 출생이라는 사실에 의하여 공동체구성원이 국가의 인적 존립조건인 국민으로 될 수 있는 실체적 자격요건이 된다. 국가의 국민이 될 수 있는 자격은 혈통과 장소를 기초로 국가의 '법'이 정하는 요건에 합치되면 당연성립하게 된다는 것이다.[11)] 헌법이 제3조 제1항에서 대한민국의 국민이 되는 요건은 법률로 "정한다" 하며, 국적법 제2조 제1항이 법이 정한 일정 요건에 해당하면 "대한민국 국민이다"라고 문구를 사용한 것을 보면 알 수 있다. 이렇게 대한민국의 국민이 되는 자격, 즉 국적은 「국적법」이 정해 주고, '국민으로서 자기식별성'을 지니는 공동체구성원이 타인과 구별될 수 있도록 공증하는 규범이 「가족관계의 등록 등에 관한 법률」과 「주민등록법」이며, 이는 적어도 공법관계에서 자기식별성을 확인해 줄 일반적인 국가적 신분확인 제도로 기능한다.[12)] 다만 2000년대 들어와 전산망 확대 및 전자정부 구축을 가능하게 하고 전 국민을 하나의 번호체계에 따라 특정하면서 효율적으로 관리하고 국가행정작용을 수행하는 기초가 되었기 때문에, 주민등록번호 폐지가 가능할 것인가 혹은 이를 대체할 제도가 있을 것인가 등의 의문도 계속된다.[13)]

현실적으로 주민등록번호 제도는 국가나 지방자치단체로 하여금 국방, 치안, 조세, 교육, 사회, 복지 등 행정사무를 신속하고 효율적으로 처리할 수 있도록 하기 위한 것으로, 궁극적으로는 주민생활 편익을 증진키 위한 것이라 볼 수 있다. 주민등록번호가 처음 도입될 당시 상황은 국민 관리나 통제 목적이 있었음을 부인할 수 없겠으나 현대 사회의 행정업무는 국방, 치안, 조세 등에 머무는 것이 아니라 참정권, 교육, 의료보험, 사회보장 등 국민 기본권 보장을 위한 다양한 영역까지 확장하고 있기에, 이러한 행정사무를 적정하고 효율적으로 처리하는 것은 국민의 기본권을 보장하고 신장시키는 데에도 중요한 의미를 지닐 것이다.[14)]

---

10) 국가인권위원회 전원위원회 결정, 주민등록번호제도 개선권고, 2014.8.5, 4-5면 참조.
11) 강경근, 헌법상 국민주권에서의 국민(Nation)의 의미, 「숭실대학교 법학논총」(제3집 1987), 143-163면 참조.
12) 강경근, 앞의 논문, 41-43면. 이러한 측면에서 오히려 이 부분은 입법 불비라고 볼 수 있다.
13) 헌법재판소 헌법재판연구원, 앞의 연구보고서, 10면.
14) 헌재 2013헌바68등, 재판관 김창종 및 재판관 조용호의 반대의견 취지.

3. 주민등록번호 보호 법제

(1) 주민등록번호에 대한 정부의 정책방향

주민등록번호 유출 및 오·남용 문제에 대한 대응의 첫 번째는 현행 주민등록번호 제도의 유지와 존속을 전제로 하되 그 사용범위와 효용을 최소화로 억제하고 주민등록번호의 불법적 활용은 엄격히 제재하는 정책이다. 두 번째는 주민등록번호 제도 자체가 지니는 문제점을 인식하고 주민등록번호 제도의 근본적 개편을 추진하는 정책이다.

[표]

	정책방향 1 주민등록번호 사용 최소화	정책방향 2 주민등록번호의 근본적 개편
주요 내용	주민등록번호 도용 금지 주민등록번호 처리 법정주의 주민등록번호 대체수단 의무화 주민번호 보호조치 강화(암호화 등) 도용·유출 시 처벌강화	주민등록번호 변경 허용 주민등록번호 체계 개편 (임의번호 도입 등)

※ 상기 구분은 국가인권위원회 김민섭 사무관의 분류이며 본고는 이를 인용한 것이다.

이렇게 주민등록번호 제도 존치를 전제로 하는 주요 정책을 「주민등록법」에 따른 주민등록번호 도용행위의 형사처벌규정, 정부와 국회의 입법 및 정책시행에 따라 추진하는 이른바 '주민등록번호 처리 법정주의' 제도를 검토한다.

(2) 주민등록번호 도용 등에 대한 제재

1990년대 인터넷 보급 등에 따라 다양한 온라인 회원제 서비스에서 개인의 손쉬운 식별과 인증을 위해 주민등록번호가 회원가입 등의 과정에서 폭넓게 사용되어 왔으나 자신의 신원이나 연령을 은닉·회피하려는 목적으로 타인의 주민등록번호를 도용하는 사례가 급격히 증가하여 왔다. 1997.12.17. 일부개정 「주민등록법」(법률 제5459호)은 다른 사람의 주민카드를 부정사용한 자를 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하였다.[15] 동 법률에서는 주민등록증을 '전자주민카드'로 전환하기 위한 점 때문에 주민등록증을 '주민카드'로 명명하였고, 타인의 주민카드 부정사용자 처벌도 전자적 주민카드로 인해 발생할 수 있는 여러 오·남용 행위를 방지하고자 하는 취지로 이해할 수 있다.[16]

---

15) 「주민등록법」(법률 제5459호) 제21조 제2항 제6호.

16) 동 법률의 제정·개정 이유를 보면 "현재 사용 중인 주민등록증은 발급된 지가 너무 오래되어 신분확인이라는 본래의 기

2001.1.26. 일부개정 「주민등록법」(법률 제6385호)은 주민등록증 또는 주민등록번호의 부정 사용행위 유형을 세분화하고 형사처벌규정을 두었다. 주민등록번호 부여 방법으로 허위의 주민등록번호를 생성하여 자기 또는 다른 사람의 재물이나 재산상의 이익을 위하여 이를 사용한 자, 허위의 주민등록번호를 생성하는 프로그램을 다른 사람에게 전달하거나 유포한 자, 다른 사람의 주민등록증을 부정사용한 자, 다른 사람의 주민등록번호를 자기 또는 다른 사람의 재물이나 재산상의 이익을 위하여 부정 사용한 자 등을 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하였다.[17)]

다만 인터넷 웹사이트에서 신규 회원가입을 하면서 주민등록번호 도용행위는[18)] '자기 또는 다른 사람의 재물이나 재산상의 이익을 위하여 부정 사용'한 것으로 보기 어려워 단순 도용자 처벌이 곤란하였다. 2006.3.24. 일부개정 「주민등록법」(법률 제7900호)은 상기 목적을 삭제하고, 단순 도용자도 형사처벌 하도록 하였다. 현행 「주민등록법」에서도 동일하게 유지되어 오고 있다. 「주민등록법」은 주민등록증이나 주민등록번호를 부정 사용한 경우에 대해서만 처벌하고 있고, 주민등록번호가 대량으로 보관·관리되고 있는 기업이나 공공기관 등에서 유출되는 등의 행위에 대해서는 처벌규정을 두고 있지 않다. 이에 대한 규제는 「개인정보보호법」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(정보통신망법) 등 일반적인 개인정보보호의 규범체계 안에서 다루어진다.

(3) 주민등록번호 처리 법정주의

주민등록번호 처리 제한을 법률에 최초로 반영한 것은 2011.3.29. 제정되어 동년 9.30.부터 시행된 「개인정보보호법」(법률 제10465호)으로 볼 수 있다. 「개인정보보호법」은 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(고유식별정보)는 원칙적으로 처리할 수 없도록 하고, 예외적으로 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우, 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용한 경우에만 처리할 수 있도록 하였다(제24조 제1항). 그리고 고유식별정보는 구체적으로 1. 주민등록번호, 2.

능을 수행함에 지장이 있고, 위·변조가 용이하여 각종 범죄에 악용되는 문제점이 있어, 종전의 주민등록증에 갈음하여 21세기 정보화시대에 대비할 수 있는 주민카드로 갱신 발급하도록 하여…" 라 하면서 "종전의 주민등록증을 주민카드로 대체"한다 하였다.

17) 「주민등록법」(법률 제6385호) 제21조 제2항 제3호, 제4호, 제8호, 제9호 참조.

18) 한국정보보호진흥원, 『2005년 개인정보 피해구제 및 상담 사례분석』, 35~36면. 이에 따르면 2005년 (당시) 한국정보보호진흥원 개인정보침해신고센터에 접수된 개인정보 침해신고·상담 민원은 총 18,206건이며 이 중 주민번호 등 타인정보의 훼손·침해·도용 민원은 9,810건으로서 전체의 53.9%를 차지하는 것으로 나타났다.

여권번호, 3. 운전면허의 면허번호, 4. 외국인등록번호를 의미한다(시행령 제19조).

이는 개인 식별 등을 목적으로 하는 일반적 개인정보는 개인정보의 활용 측면을 고려하여 본인의 동의 외에도 비교적 폭넓은 수집·이용을 허용하는데 반해, 주민등록번호를 비롯한 고유식별정보는 정보주체의 별도 동의 및 법령의 구체적 요구·허용 외에는 처리를 불허함으로써 주민등록번호의 무분별한 활용을 억제해보려는 취지임을 알 수 있다. 주민등록번호는 「개인정보보호법」 제정 당시 이미 도용 및 유출 사례가 사회적 위기감을 주고 있어 법률이 그 처리에 엄격한 규정을 둔 것이다. 다만 그 외 여권번호, 운전면허번호, 외국인등록번호 등까지 고유식별정보 범위에 모두 포함시켜 규제할 필요가 있는지는 의문이 있었다.[19]

주민등록번호 법정주의가 처음으로 반영된 것은 주민등록번호 도용이 주로 문제되는 정보통신 분야를 규율하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(정보통신망법)의 개정을 통하여서다. 2012.2.17. 일부개정된 정보통신망법(법률 제11322호)는 1. 본인확인기관으로 지정받은 경우 2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우를 제외하고는 정보통신서비스 제공자는 이용자의 주민등록번호를 수집·이용할 수 없도록 하였다(제23조의2 제1항).

이어서 「개인정보보호법」(법률 제11990호 2013.8.6. 일부개정)에서도 주민등록번호 처리 법정주의가 도입되었다. 「개인정보보호법」은 원칙적으로 사회 전 분야 개인정보처리자에 적용되는 법률이므로, 동 법률에 주민등록번호 처리 법정주의가 도입된 것은 온·오프라인 등을 불문하고 사회 전 분야에서 불필요한 주민등록번호 수집을 금지하게 한 의미가 있다.[20] 즉 「정보통신망법」에 의한 법정주의는 민간 정보통신서비스 제공자(사업자)에 한하여 적용되는 것임에 반해, 「개인정보보호법」에 따른 주민등록번호 처리 법정주의는 원칙적으로 중앙행정기관, 지방자치단체, 공공기관, 민간기업·단체 등을 막론하고 모두 적용되게 되므로 그 파급효과가 매우 커진다. 즉 여타의 고유식별정보(여권번호, 운전면허의 면허번호, 외국인등록번호)는 정보주체의 별도 동의가 있으면 처리가 가능한데 비해(제24조 제1항) 주민등록번호만큼은 정보주체의 별도 동의를 받아 처리했다고 하더라도 불법이 되며, 반드시 법령의 구체적 요구·허용 근거가

19) 김민섭, 「개인정보의 보호와 활용의 조화에 관한 법제적 연구」(숭실대학교대학원 박사학위논문 2014), 211~212면 참조. 개인정보보호법 제정 당시 전 사회적으로 도용이나 유출 문제가 빈발하였던 것은 고유식별정보 중에서 주민등록번호뿐이며 그 외 여권번호, 운전면허번호 등의 대량유출사고는 거의 알려진 바 없다. 또 법안제정과정 연구자료 등에 고유식별정보 처리기준의 입법필요성은 전부 주민등록번호에 대한 설명이고 고유식별정보는 사례조차 소개되지 않음을 볼 수 있다(행정안전부 발간 「개인정보 보호법령 및 지침고시 해설」(2011)에서도 같다).

20) 안전행정부, 『주민등록번호 수집 금지 제도 가이드라인』(2014.1), 4면.

있어야만 주민등록번호를 처리할 수 있게 된 것이 가장 큰 차이점이다.

2016.3.29. 개정되어 2017.3.30. 시행 예정인 「개인정보보호법」(법률 14107호)은 주민등록번호 처리 법정주의를 강화하였다. 즉 주민등록번호의 처리 허용요건으로 이전에는 "법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우"라고 규정하던 것을 "법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우"로 한정하여[21] 이전에 문제로 지적되던 '시행규칙 상의 주민등록번호 처리근거'는 배제하였다.[22]

Ⅱ. 주민등록번호 법제의 헌법재판소 결정

1. 헌법재판소 결정의 배경 – 주민등록번호 변경의 가부

주민등록번호는 고유불변성, 일신종속성, 종신성 등을 기본 속성으로 하고 있어, 「주민등록법」은 주민등록번호 정정(訂正) 등 '변경'을 기본적으로 인정하지 않으며, 주민등록사항 정정이 있거나 주민등록번호 오류가 있는 경우에 한하여 '정정'을 규정하고 있을 뿐이다.[23] 예외적으로 북한이탈주민의 경우 신변보호 차원에서 예외적으로 1회에 한하여 주민등록번호의 정정 신청이 가능하다.[24] 주민등록번호 불변성, 일신전속성은 주민등록번호 제도의 근간을 이루는 고유한 성격이다. 다만 주민등록번호 도용으로 지속적 피해를 입고 있는 자 등에 대해서는 제한적 범위 내에서 그 변경을 허용할 필요가 있다는 견해가 다수 제시된 바 있다.

국가인권위원회는 수차에 걸쳐 주민등록번호가 내포하는 문제요인을 인지하고 주민등록번호 변경 허용 등을 권고하여 왔다.[25] 주민등록제도의 주무부처인 행정자치부, 기타 개인정보보호 관련 정부 부처에서도 주민등록번호를 포함한 대량 개인정보 유출 사건이 연이어 발생하면서 그 대응책의 하나로 주민등록번호 변경 부분허용의 필요성을 인정하고 있다.[26]

---

21) 「개인정보보호법」(법률 제14107호) 제24조의2 제1항 제1호.

22) 행정자치부 보도자료, "주민등록번호 보호제도 한층 강화된다", 2016.3.11 참조. 이에 따르면 시행규칙에 주민등록번호 수집근거를 둔 경우가 아직 464개에 달하고 있어 1년간 법 시행 유예기간을 둔 것이며, 행정자치부는 법 시행 이전까지 시행규칙을 일제히 정비할 계획임을 밝히고 있다.

23) 「주민등록법」 제13조, 제14조 제1항 및 제3항. 「주민등록법」 시행령 제8조 제1항, 제4항

24) 「북한이탈주민의 보호 및 정착지원에 관한 법률」 제19조의3(주민등록번호 정정의 특례).

25) 국가인권위원회, 『정보인권 보고서』(2013.1), 41-42면; 국가인권위원회 보도자료, "주민등록번호, 이제는 전면 개편해야", 2014.8.8 참조.

26) 관계부처 합동, 『개인정보보호 정상화 대책』(2014.7), 20면 참조.

이런 상황에서, 헌법재판소는 2015년 12월 23일 선고한 2013헌바68, 2014헌마449(병합) 결정에서 개인별로 주민등록번호를 부여하면서 주민등록번호 변경에 관한 규정을 두고 있지 않은 「주민등록법」 제7조는 개인정보자기결정권을 침해한다고 결정함으로써 주민등록번호 변경 허용과 관련한 논의에 방점을 찍게 되었다. 이하에서는 헌법재판소의 동 결정에 대한 사건 개요와 주요 내용을 살펴보고 그 시사점을 논의해보기로 한다.

2. 주민등록법 제7조 헌법불합치결정(헌재 2015.12.23. 2013헌바68, 2014헌마449(병합))

(1) 사건의 개요

헌법불합치결정은 두 청구 사건의 병합 결정이다.

2013헌바68 사건의 청구인들은 개인정보 유출 또는 침해사고로 주민등록번호가 불법 유출되었다는 이유로 각 관할 지방자치단체장에게 주민등록번호 변경을 신청하였으나 현행 「주민등록법」 상 주민등록번호 불법 유출을 원인으로 한 변경은 허용되지 않는다는 이유로 변경 거부 통지를 받았다. 청구인들은 주민등록번호 변경신청 거부처분 취소의 소를 제기하였으나[27] 같은 이유로 각하되자 이에 불복, 항소[28] 제기 및 주민등록법 제7조제3항, 제4항 등이 헌법 위반임을 주장하며 위헌법률심판제청을 신청하였으나[29] 항소 기각과 동시에 위 위헌법률심판제청신청도 각하되자 이 사건 헌법소원심판을 청구하였다.

2014헌마449 사건의 청구인들은 2014년 1월경 발생한 신용카드 회사의 개인정보 유출사고로 인하여 주민등록번호가 불법 유출되었다는 이유로 각 관할 지방자치단체장에게 주민등록번호 변경을 신청하였으나 현행 「주민등록법」 상 주민등록번호 불법 유출을 원인으로 한 변경은 허용되지 않는다는 이유로 변경 거부 통지를 받았다. 이에 청구인들은 주민등록법 제7조제3항, 제4항, 주민등록법 시행령 제7조제4항, 제8조제1항 및 주민등록법 시행규칙 제2조에서 불법 유출된 주민등록번호에 대한 변경절차를 두고 있지 않은 것이 청구인들의 기본권을 침해한다고 주장하며 이 사건 헌법소원심판을 청구하였다.

27) 서울행정법원 2012구합1204.
28) 서울고등법원 2012누16727.
29) 서울고등법원 2012아506.

(2) 결정의 주요 내용과 형식

① 심판대상

청구인들의 주장에 따르면, 심판대상조항에서 주민등록번호가 불법 유출된 경우 등과 같이 주민등록번호의 잘못된 이용에 대비한 '주민등록번호의 변경'에 대하여 아무런 규정을 두고 있지 아니한 것은 개인정보자기결정권을 침해하는 것이라고 주장하였다.[30] 이 사건 다수의견은 청구인들이 주장하는 것은 위 조항들의 내용이 위헌이라는 것이 아니라 주민등록번호의 잘못된 이용에 대비한 '주민등록번호 변경'에 대하여 아무런 규정을 두고 있지 않은 것이 헌법에 위반된다는 것이므로 이는 주민등록번호의 변경에 대하여 아무런 규정을 두지 아니한 부진정 입법부작위가 위헌이라는 것이며, 따라서 청구인들의 주장과 가장 밀접하게 관련되는 주민등록법 제7조 전체를 심판대상으로 삼았다.

② 제한되는 기본권

개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인을 식별할 수 있게 하는 일체의 정보라고 할 수 있다. 이러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.[31] 주민등록번호는 당해 개인을 식별할 수 있는 정보에 해당하는 개인정보이며, 심판대상조항이 국가가 주민등록번호를 부여·관리·이용하면서 그 변경에 관한 규정을 두지 않음으로써 주민등록번호 불법 유출 등을 원인으로 자신의 주민등록번호를 변경하고자 하는 청구인들의 개인정보자기결정권을 제한하고 있다고 보았다.

③ 헌법불합치결정과 잠정적용명령

헌법재판소는 부작위의 위헌성을 이유로 심판대상조항에 대해 단순위헌결정을 할 경우 주민등록번호 제도 자체에 관한 근거규정이 사라지게 되어 용인하기 어려운 법적 공백이 생기게 되므로 심판대상조항에 대하여 단순위헌결정을 하는 대신 헌법불합치결정을 선고하되, 입법자의 개선입법이 이루어질 때까지 계속적용을 명하기로 하며, 입법자는 2017. 12. 31.까지는 개

30) 2013헌바68 사건 청구인들은 주민등록법 제7조제3항, 제4항을, 2014헌마449 사건 청구인들은 주민등록법 제7조제3항, 제4항, 주민등록법 시행령 제7조제4항, 제8조제1항, 주민등록법 시행규칙 제2조를 각 심판대상조항으로 삼고 있다.

31) 헌재 2005.5.26, 99헌마513등.

선입법을 이행해야 하고, 그때까지 개선입법이 이루어지지 않으면 심판대상조항은 2018. 1. 1. 부터 효력을 상실한다고 하였다.

(3) 개인정보자기결정권의 침해 여부에 대한 헌재 결정

헌법재판소는 “주민등록번호제도는 주민등록제도의 일부로서 주민에게 주민등록번호를 부여하여 오늘날 국가나 지방자치단체로 하여금 국방, 치안, 조세, 사회복지 등의 행정사무를 신속하고 효율적으로 처리할 수 있도록 하며, 심판대상조항이 모든 주민에게 고유한 주민등록번호를 부여하면서 이를 변경할 수 없도록 한 것은 주민생활의 편익을 증진시키고 행정사무를 신속하고 효율적으로 처리하기 위한 것으로서 그 입법목적의 정당성과 수단의 적합성을 인정할 수 있다”고 보았다.

그러나 “현재의 주민등록번호는 목적별로 식별번호를 구분하여 사용하지 않고 모든 영역에 걸쳐 통합 사용되고 있는 바 (중략) 이를 관리하는 국가는 주민등록번호가 유출되거나 악용되는 사례가 발생하지 않도록 철저히 관리하여야 하며, 그럼에도 불구하고 문제가 발생하는 경우 그로 인한 피해가 최소화되도록 제도를 정비하고 보완하여야 할 의무가 있다”고 하면서, 특히 “실제 유출된 주민등록번호가 다른 개인정보와 연계되어 각종 광고 마케팅에 이용되고 사기, 보이스피싱 등의 범죄에 악용되는 등 해악이 현실화되고 있음은 신문이나 방송을 통하여 쉽게 목도할 수 있다”고 지적하면서, “이러한 현실에서 주민등록번호 유출 또는 오·남용으로 인하여 발생할 수 있는 피해 등에 대한 아무런 고려 없이 주민등록번호 변경을 일률적으로 허용하지 않는 것은 그 자체로 개인정보자기결정권에 대한 과도한 침해가 될 수 있다”고 하였다. 또한 “비록 국가가 개인정보보호법이나 정보통신망법 등의 입법을 통하여 (중략) 주민등록번호의 유출이나 오·남용을 예방하는 조치를 취하고 있다고는 하나, (중략) 이미 주민등록번호가 유출되어 발생하였거나 발생할 수 있는 피해 등에 대해서는 뚜렷한 해결책을 제시하지 못하고 있”다고 지적하고 있다.

한편 개별적인 주민등록번호 변경을 허용할 경우 주민등록번호의 개인식별기능과 본인동일성 증명기능이 약화되어 주민등록제도 목적달성이 어렵게 되고 이를 불순한 용도로 악용하려는 경우가 생길 수 있으나, “주민등록번호가 변경된다고 하더라도 변경 전 주민등록번호와의 연계 시스템을 구축하여 활용한다면 본인확인이 가능할 것”이고, “입법자가 정하는 일정한 요건을 구비한 경우에 객관성과 공정성을 갖춘 행정기관 또는 사법기관의 심사를 거쳐 변경을 할 수 있도록 허용한다면” 큰 혼란을 불러일으키지 않을 것으로 보았다.[32]

따라서 다수의견은 심판대상조항이 모든 주민에게 고유한 주민등록번호를 부여하면서 주민등

록번호 유출이나 오·남용으로 인하여 발생할 수 있는 피해 등에 대한 아무런 고려 없이 일률적으로 이를 변경할 수 없도록 한 것은 침해의 최소성 원칙에 위반된다고 보았다.

결과적으로 다수의견은 "일률적으로 주민등록번호를 변경할 수 없도록 함으로써 침해되는 주민등록번호 소지자의 개인정보자기결정권에 관한 사익은 심판대상조항에 의하여 달성되는 (행정사무의 신속하고 효율적인 처리를 통한) 구체적 공익에 비하여 결코 적지 않다고 하여 법익의 균형성도 충족하지 못한 것으로 보았다. 따라서 헌법재판소는 주민등록번호 변경에 관한 규정을 두고 있지 않은 심판대상조항은 과잉금지원칙을 위반하여 청구인들의 개인정보자기결정권을 침해한다고 결정하였다.

3. 헌법재판소 결정의 의의와 법제개선안

헌법재판소 결정은 현행 주민등록번호 제도가 내포하는 주민생활의 편익 증진과 행정사무의 적정한 처리 도모 및 국방, 치안, 조세, 사회복지 등의 행정사무를 신속·효율적으로 처리할 수 있도록 하는 헌법합치적 긍정적 기능을 인정함과 동시에, 정보사회 진전 및 스마트·미디어 시대 진입에 따른 주민등록번호 등 개인정보 대량 유출과 도용으로 인한 문제점과 한계를 명확히 인식하고 향후의 입법적 조치까지 고려하여 개인정보자기결정권의 보호를 위한 개선책을 제시하는 등 균형조화적 입장을 채택하였다.

주민등록번호 변경 허용 취지의 「주민등록법」 개정이 문제되는 바, 국회와 정부는 헌법재판소의 주민등록법 제7조에 대한 헌법불합치 결정이 나오기 이전부터, 일정 요건 하에서 주민등록번호의 변경을 허용하는 등의 법률 개정안을 발의해온 바 있다.

사견으로는 아직 헌법재판소가 권고한 2017년 12월 31일까지 비교적 충분한 시간적 여유가 있으므로 제20대 국회 개원 후 충분한 토론과 논의를 거쳐 「주민등록법」을 개정하는 것이 좀 더 바람직하지 않을까 생각한다.

32) 다수의견은 그 증례로서, 공인인증서(NPKI)나 전자관인(GPKI)이 1년 내지 2년마다 갱신되어야 하지만 개인식별기능에 별다른 문제가 발생한 바 없다는 점, 2010년 전후로 한해 평균 16만 1천여 명이 개명을 신청하고 그 인용률은 94.1%에 이르지만 이로 인한 사회적인 혼란이 일어나지는 않았다는 점을 들고 있다.

Ⅲ. 헌법재판소 결정의 평가

1. 심판대상조문 확대확정 관련

2013헌바68 사건 청구인들은 주민등록법 제7조제3항, 제4항, 2014헌마449 사건 청구인들은 주민등록법 제7조제3항, 제4항, 주민등록법 시행령 제7조제4항, 제8조제1항, 주민등록법 시행규칙 제2조를 심판대상으로 청구하였다. 다수의견은 청구인들의 주장은 위 조항들의 내용이 위헌이라는 것이 아니라 주민등록번호의 잘못된 이용에 대비한 주민등록번호 변경에 대하여 아무런 규정을 두고 있지 않은 이른바 '부진정 입법부작위'가 위헌이라는 것이며, 따라서 청구인들의 주장과 가장 밀접하게 관련되는 주민등록법 제7조 전체를 심판대상으로 삼았다. 헌법재판소는 일찍이 "부진정입법부작위를 대상으로, 즉 입법의 내용·범위·절차 등의 결함을 이유로 헌법소원을 제기하려면 이 경우에는 결함이 있는 당해 입법규정 그 자체를 대상으로 하여 그것이 평등의 원칙에 위배된다는 등 헌법위반을 내세워 적극적인 헌법소원을 제기"해야 한다는 기준을 천명한바 있다.[33]

재판관 이진성의 반대의견은 "청구인들이 입법부작위라고 주장하는 주민등록번호의 변경은 주민등록번호 제도 그 자체가 아니라 주민등록번호의 부여 방법에 관한 구체적 내용으로 보는 것이 상당하므로, 그 근거규정인 주민등록법 제7조 제4항을 심판대상조항으로 삼아야 한다"고 보았다. 즉 "주민등록법 제7조 제4항의 위임을 받아 마련된 주민등록법 시행령 제8조에서 주민등록번호가 부여된 이후 그 잘못된 기재를 바로잡는 '주민등록번호의 정정'을 규정하고 있는 점에 비추어도 사후적으로 주민등록번호를 고치는 제도로서 '주민등록번호의 변경'은 주민등록법 제7조 제4항에 의한 '주민등록번호의 부여 방법'의 범주 내에 있는 것으로 볼 수 있다"고 보면서, "다수의견의 가장 근본적인 문제는 주민등록법 제7조 모두에 대한 헌법불합치 결정의 효력으로 주민등록번호 제도뿐만 아니라 청구인들이 심판대상으로 청구하지도 아니한 주민등록표 제도에 관해서까지 법적 공백과 혼란이 발생할 가능성이 있다는 것이다"라는 의견을 개진하였다.

헌법재판소가 본 사건과 관련하여 심판대상조문으로 확대한「주민등록법」제7조를 보면, 제1항은 개인별 및 세대별 주민등록표의 작성에 관한 원칙, 제2항은 개인별·세대별 주민등록표의 내용과 방법, 제3항은 주민등록번호 부여의 근거, 제4항은 주민등록번호 부여 방법의 위임으로 볼 수 있다.[34] 따라서 다수의견과 같이「주민등록법」제7조 전체로 심판대상을 확대할

33) 헌재 1996.10.31. 94헌마108,『판례집』(8-2), 489면.

경우 (심판대상으로 청구되지도 않은) 주민등록표 제도 그 자체의 위헌성을 인정하는 결과가 되므로[35], 본 사건에서 부진정입법부작위를 대상으로 한 청구는 '주민등록번호'의 근거와 그 부여방법에 대한 「주민등록법」 제7조 제3항 및 제4항으로 한정하는 것이 순리적 판단이었으리라 본다.[36]

2. 주민등록번호 변경허용과 개인정보자기결정권

헌법재판소는 2005. 5. 26. 99헌마513, 2004헌마190(병합) 결정에서 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리를 말한다고 판시하였다. 그리고 개인정보자기결정권의 헌법상 근거로 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권, 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있다고 하면서, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이며 (중략) 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권으로 보고 있다.[37]

생각건대 모든 국민은 사생활의 비밀을 침해받지 않는다 하는 헌법 제17조 전단은 소극적 방어권인 프라이버시권(the right of privacy)이며, 사생활의 자유를 침해받지 않는다 하는 후단은 개인영역의 적극적 형성권인 자기결정권(the right of self-determination)으로서 이는 헌법 제10조 행복추구권의 일반적 행동자유권에서도 근거한다고 봄이 타당하다 하겠다.[38] 헌법재판소는 본 사건 결정에서 주민등록번호는 당해 개인을 식별할 수 있는 정보에 해당하는 개인정보이며, 따라서 심판대상조항이 국가가 주민등록번호를 부여・관리・이용하면서 그 변경

34) 「주민등록법」 제7조(주민등록표 등의 작성) ①시장·군수 또는 구청장은 주민등록사항을 기록하기 위하여 전산정보처리조직(이하 "전산조직"이라 한다)으로 개인별 및 세대별 주민등록표(이하 "주민등록표"라 한다)와 세대별 주민등록표 색인부를 작성하고 기록·관리·보존하여야 한다. ②개인별 주민등록표는 개인에 관한 기록을 종합적으로 기록·관리하며 세대별(世帶別) 주민등록표는 그 세대에 관한 기록을 통합하여 기록·관리한다. ③시장·군수 또는 구청장은 주민에게 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다. ④주민등록표와 세대별 주민등록표 색인부의 서식 및 기록·관리·보존방법 등에 필요한 사항과 주민등록번호를 부여하는 방법은 대통령령으로 정한다.

35) 특히 「주민등록법」 제7조 제1항·제2항 및 이의 위임을 받은 「주민등록법」 시행령 제6조가 그러하다.

36) "주민등록번호에 대한 직접적 규정은 청구인들의 주장과 같이 주민등록법 제7조 제3항, 제4항 등이며, 직접적으로 침해되는 법령은 시행령 제7조, 제8조인 것을 간과해서는 아니된다". 손형섭, 주민등록법 제7조 헌법불합치결정에 관한 연구, (한국헌법학회·국가인권위원회 공동주최 제89회 정기학술대회) 「'주민등록번호와 개인인증시스템의 헌법적 검토' 발표자료집」(2016.3,), 10-11면.

37) 헌재 2005.5.26. 99헌마513등, 『판례집』(17-1), 683면.

38) 강경근, 『일반헌법학』(법문사 2014), 397면.

에 관한 규정을 두지 않음으로써 주민등록번호 불법 유출 등을 원인으로 자신의 주민등록번호를 변경하고자 하는 청구인들의 개인정보자기결정권을 제한하고 있다고 보았다.

재판관 김창종, 재판관 조용호의 반대의견은 "주민등록번호의 개별적인 변경을 인정하는 경우에는 주민등록번호의 개인식별기능이 약화되어 주민등록번호 제도의 입법목적 달성이 어렵게 된다"고 하면서 국가안보차원에서 국민의 정확한 신원확인의 필요성, 범죄은폐·탈세·채무면탈 또는 신분세탁 등의 불순한 용도로 이를 악용하는 경우가 발생할 우려, 주민등록번호 변경에 따른 각종 기록의 정정·변경 등 막대한 사회적 비용 발생 등을 예시하고 있다. 또한 입법자가 개인에게 주민등록번호 변경신청권을 인정하지 않는 대신 주민등록번호 부정사용에 대한 형사처벌[39], 개인정보처리자 또는 정보통신사업 제공자 등의 주민등록번호 수집·이용 제한[40], 주민등록번호의 대체수단 제공 의무화[41] 및 이의 위반시 과태료 부과[42], 주민등록번호의 분실·도난·유출·변조·훼손된 경우 개인정보처리자에게 5억원 이하의 과징금 부과·징수[43], 개인정보 유출 등에 대한 피해구제를 강화하고자 징벌적 손해배상 및 법정 손해배상 제도 도입[44] 등 여러 입법을 통해 주민등록번호 유출 등에 대한 사전적 예방과 사후적 제재 및 피해구제 조치를 강구하고 있음을 지적하면서, 이러한 점들을 종합적으로 고려할 때 심판대상조항이 주민등록번호의 변경에 대한 규정을 두고 있지 아니한 것이 침해최소성의 원칙에 반한다 보기 어렵다는 입장을 취하였다. 또한 주민등록의 대상인 주민에게 주민등록번호 변경을 허가하지 않음으로써 달성할 수 있게 되는 공익이 그로 인한 정보주체의 불이익에 비하여 결코 더 작다고 보기는 어려울 것이므로 법익균형성의 원칙에도 반하지 않는다 보면서, 심판대상조항이 주민등록번호 변경에 관한 규정을 두고 있지 않은 것이 과잉금지원칙을 위반하여 개인정보자기결정권을 침해한다고 볼 수 없다 하였다.

생각건대, 헌법 제17조의 사생활의 비밀과 자유는 사생활영역을 방해받지 아니할 소극적 방어권임과 동시에 개인적 존재영역을 구체적·능동적으로 형성·실현하는 자기결정권을 주관적 공권으로 하는 헌법상 권리로 파악하여야 할 것이다.[45] 국민은 헌법에 근거한 대국가적 청구권을 행사하여 개인의 자유를 국가로부터 방어하고 침해를 배제·예방하는 소극적 권리를 가짐은 물론 국가에 일정 급부의 제공을 요구할 수 있는 적극적 권리도 향유한다.[46] 따라서 개인정보

39) 「주민등록법 제37조 제9호, 제10호.
40) 「개인정보 보호법」 제24조의2 제1항, 「정보통신망법」 제23조의2 제1항.
41) 「개인정보 보호법」 제24조의2 제2항, 「정보통신망법」 제23조의2 제2항.
42) 「개인정보 보호법」 제75조 제2항 제4의2호, 제5호, 「정보통신망법」 제76조 제1항 제2호.
43) 「개인정보 보호법」 제34조의2.
44) 「개인정보 보호법」 제39조, 제39조의2.
45) 강경근, 앞의 책, 397면.

자기결정권은 사생활의 평온을 침해받지 아니하고 내밀한 사적 영역이 원치 않게 공표·노출되지 아니하도록 하는 소극적 침해배제청구권(방어권)인 동시에, 스스로의 존재나 영역을 구체적으로 형성·실현하는 것, 즉 자신에 관한 개인정보의 수집·활용을 허락하거나 또는 거부하는 행위, 개인정보의 제3자적 제공이나 유통을 허락하거나 거부하는 행위, 자기 자신의 개인정보에 대한 열람 및 정정·삭제 등을 요구함으로써 개인정보의 완전성·무결성을 추구하는 등 자기결정권을 적극적으로 요구·실현하는 주관적 공권으로 이해하여야 할 것이다.[47]

이러한 시각에서 볼 때, 입법자가 「개인정보보호법」 및 「정보통신망법」 등의 제반 조치를 통해 주민등록번호 도용·유출에 대한 사전적, 사후적 제재조치를 마련하고 있다고는 하나, 이와는 별도로 일단 한번 주민등록번호가 유출·도용된 정보주체 당사자는 그 주민등록번호의 변경 조치 외에는 계속된 피해를 입을 수밖에 없는 위치에 놓이게 된다. 따라서 보다 근본적인 개인정보자기결정권의 실현을 위해서는 다수의견과 같이 주민등록번호의 변경을 허락하는 것이 침해의 최소성의 원칙을 충족한다고 보아야 할 것이다.

3. 주민등록번호 변경허용과 주민번호 기능약화

본 결정 다수의견은 개별적인 주민등록번호 변경을 허용할 경우 주민등록번호의 개인식별기능과 본인동일성 증명기능이 약화되어 주민등록제도 목적달성이 어렵게 될 우려에 대해, 변경 전 주민등록번호와의 연계 시스템 구축·활용, 객관성과 공정성을 갖춘 행정기관 또는 사법기관의 심사를 거친 변경 등을 대안으로 제시하고 있다. 이러한 보완 절차는 앞서 살펴 본 국가인권위원회의 권고 등에서도 대안으로 언급된 바 있으며[48] 당연히 필요한 부분임에 공감하는 바이다. 다만 다수의견은 주민등록번호 변경이 허용되더라도 공인인증서(NPKI)나 전자관인(GPKI)의 1~2년 주기 갱신에도 불구하고 개인식별기능에 별다른 문제가 발생한 바 없었다거나, 개명신청 및 인용이 상당수에 이르지만 이로 인한 사회적 혼란이 일어나지 않았다는 것을 예로 들어 별다른 문제가 없을 것임을 밝히고 있으며, "특히 이 부분은 실제 본 사건의 공개변론에서 청구인 측이 중요하게 다룬 분야로 헌법재판소의 결정문에 그대로 인용되었다"는 주장[49]도 제기되고 있다.

---

46) 강경근, 앞의 책, 217면.
47) 김민섭, 앞의 논문, 44면.
48) 국가인권위원회, 앞의 보고서, 41-42면.
49) 이혜정, 헌법재판소 주민등록법 위헌 결정의 의의, (민주사회를위한변호사모임 등 주최 토론회) 「'주민등록번호제, 어떻게 개편할 것인가' 발표자료집」(2016.1). 16면 참조.

성명은 개인이 선택하는 것이고[50] 「가족관계의 등록 등에 관한 법률」에 따른 출생신고 등이 있을 때 그에 따라 가족관계등록부 및 주민등록사항에 등록·기재되는 것인 반면, 주민등록번호는 국가가 주민의 신고에 의하여 일정 법칙에 따라 (강제로)생성·부여하는 것으로 양자는 근본적 차이가 있다. 또한 성명은 주민등록번호와 달리 동명이인이 존재할 수 있으며[51], 개인을 표상하는 가장 중요한 개인정보이기는 하나 이는 다른 개인정보 항목과 결합되어 그 의미를 가지는 것이지 성명 그 자체로 개인정보 통합 연결자(key data) 또는 일차키(primary key)로는 잘 사용되지 않는다.[52]

공인인증서의 경우에도 통산 1년 주기로 갱신이 이루어지고 있으며 그에 따른 혼란이 발생하지 않음은 다수의견에서 적시된 바와 같으나, 공인인증서의 갱신이란 사실상 그 유효기간[53]을 새로 정하는 것에 불과하지 '특정인의 공인인증서'라는 근본적인 법적 성격이 변화하는 것은 절대 아니다. 무엇보다 공인인증서(NPKI, GPKI)를 신규 발급하는 경우에는 발급받고자 하는 자의 신원을 성명 및 주민등록번호 등에 의해 확인하고 그에 기하여 발급된다는 점, 즉 공인인증서 제도 또한 주민등록번호에 기반한 제도임을 간과한 것으로 보인다.[54] 따라서 단순히 성명이나 공인인증서의 변경 허용 사례를 주민등록번호의 변경 허용에 따른 문제가 없을 것이라는 근거로 삼는 것은 타당치 않다. 주민등록번호는 다른 개인정보 항목과는 그 일신전속성, 식별성, 유일성 등에서 궤를 달리하는 개인정보이므로 주민등록번호의 변경은 엄격한 요건을 구비한 경우에 한해 철저한 심사를 거쳐 허용하도록 정교한 기준과 절차를 갖출 것이 반드시 요구되어야 할 것이다.

---

50) 헌재 2015.12.23. 2013헌바68등, 『판례집』(27-2하), 495면, 재판관 김창종, 조용호의 반대의견 참조.

51) 주민등록번호는 발급원리상 '동번이인'이 허락되지 않는다. 다만 기재 실수 등이 극소수 존재할 수 있다.

52) 전산의 측면에서, 데이터베이스(database)를 구축하는 경우 일차키(primary key)의 가장 핵심적 요건은 unique성, 즉 유일성·독자성을 갖추어야 한다.

53) 「전자서명법」 제15조(공인인증서의 발급) ①(생략) ②공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다. 5. 공인인증서의 유효기간

54) 「전자서명법」 제15조(공인인증서의 발급) ①공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다. 이 경우 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하여야 한다. 「전자서명법」 시행규칙 제13조의2(신원확인의 기준 및 방법) ①공인인증기관은 법 제15조제1항 후단의 규정에 의하여 공인인증서를 발급받고자 하는 자의 신원을 확인하는 경우에는 다음 각호의 구분에 따른 실지명의를 기준으로 하여야 한다. 1. 개인의 경우 가. 주민등록표에 기재된 성명 및 주민등록번호. 다만, 재외국민의 경우에는 여권에 기재된 성명 및 여권번호(여권이 발급되지 아니한 재외국민의 경우에는 「재외국민등록법」에 의한 등록부에 기재된 성명 및 등록번호) (이하 생략)

참고문헌

강경근, 『일반헌법학』(법문사 2014).

강경근, 주민등록과 전산화 그리고 프라이버시, 「아·태공법연구」(제4집 1997).

강경근, 헌법상 국민주권에서의 국민(Nation)의 의미, 「숭실대학교 법학논총」(제3집 1987).

개인정보보호위원회, 『2015 개인정보보호 연차보고서』(2015.8).

고문현 외, 『국가신분확인체계 발전방안연구』(행정안전부 연구용역보고서 2010).

고문현, 주민등록제도의 문제점과 개선방안, 「공법학연구」(제13권제4호 한국비교공법학회 2012.11).

관계부처 합동, 『개인정보보호 정상화 대책』(2014.7).

관계부처 합동, 『금융분야 개인정보 유출 재발방지 종합대책』(2014.3).

국가인권위원회, 『정보인권 보고서』(2013.1).

국회도서관, 『개인식별번호(주민등록번호)에 관한 외국입법례』(2014.4).

김민섭, 『개인정보의 보호와 활용의 조화에 관한 법제적 연구』(숭실대학교 대학원 박사학위논문 2014).

김민호, 정보사회에서 주민등록제도와 개인식별번호체계의 공법적 쟁점, 「공법연구」(제40집 제1호 한국공법학회 2011.10).

김민호 외, 『주민등록번호제도 개선방안연구』(국가경쟁력강화위원회 연구용역보고서 2009.11).

김주영, 「주민등록법」의 개정방향에 관한 소고 -주민등록번호 변경제도를 중심으로-, (한국헌법학회·국가인권위원회 공동주최) 「제89회 정기학술대회 발표자료집」(2016.3).

민병조·김민섭 외, 『금융소비자보호』(한국금융연수원 2014).

손형섭, 주민등록법 제7조 헌법불합치결정에 관한 연구, (한국헌법학회·국가인권위원회 공동주최) 「제89회 정기학술대회 발표자료집」(2016.3).

안전행정부, 『주민등록번호 수집 금지 제도 가이드라인』(2014.1).

이장희, 개인식별수단의 헌법적 한계와 주민등록번호의 강제적 부여의 문제점 검토, 「고려법학」(제69호 고려대학교 법학연구원 2013.6).

이혜정, 헌법재판소 주민등록법 위헌 결정의 의의, (민주사회를위한변호사모임 등 주최 토론회) 「'주민등록번호제, 어떻게 개편할 것인가' 발표자료집」(2016.1).

하혜영, 주민등록번호의 변경에 대한 논의와 과제, 「이슈와 논점」(제914호 국회입법조사처 2014.10).

Korea's Personal Identification Number Law's present condition and drawbacks

Ⅰ. Present Condition of Resident Registration Number Law

1. Concept, origin, and dysfunction of Resident Registration Number

(1) Resident Registration Number's concept and grant system

The Representative Personal Identification Number Law System of Korea is the Resident Registration Number Law based on the 'Resident Registration Number'. Resident Registration Number was first introduced in 1968; since 1975, it adopts the function to identify individuals efficiently. Since the advancement of information-based era in the 1990's, Resident Registration Number has expanded its usage in individuals identification and confirmation through on-line. This report discusses the present conditions and drawbacks of Resident Registration Number based on cases of Constitutional Court.

(2) Resident Registration Number's Introduction Background and Origin

Resident Registration Number is formed with two sets of 6 digits and 7 digits, connected by "-" based on Personal Resident Registration Number Law(Article 3 Section 1), 1 Resident Registration Number per person(Section 3). The First 6 digits indicates the birth information. the 7 digits indicates: sex(male 1, female 2), birth-decade, area code, reporting order, and check digits. Since Jan. 26 2001 Resident Registration Number Law (Legislation 6385) "Mayor/governor or chief of Gu(구) district must grant a distinct registration number to individual residents"(Article 7 Section 3), the grant of Resident Registration Number was officially legislated.

(3) Resident Registration Number's Dysfunction and the Decision of Constitutional Court.

The dysfunction of Resident Registration Number system is that, it does not have a proper prevention system or subsequent remedial measures for leaked personal information and identity

thefts, because the current legislation does not allow to change the Resident Registration Number. The Constitutional Court made the decision on Dec. 23 2015. (헌바68, 2014헌마449(병합))

2. Constitutional Function of Resident Registration Number .

To identify the individuals identity by granting personal identification serial numbers, Resident Registration Number's function is to identify residential administration, general standard information, confirmation functions, connecting functions, descriptions, and etc. of an individual. However, since the Resident Registration Number is formed with individual's personal information such as: birth date, sex and etc., Resident Registration Number discloses individual's personal information before the individual's consent. Due to these privacy matters, Resident Registration Number system must be reconsidered if it's a proper system within the Constitutional Law.

3. Resident Registration Number Protection Legislation.

(1) Government's Policy Direction for Resident Registration Number.

Examining the Prescribed criminal punishment of identity theft through Resident Registration Number and 'Resident Registration Number Handling Law' which the government and congress are legislating according to the Resident Registration Law.

(2) Sanctions for Resident Registration Number Identity Thefts.

Resident Registration Law only penalizes when Resident Registration Number or Resident Registration Number ID card is falsely used. There are no rules of punishment for corporations and public institutions when Resident Registration Number information is leaked, even though large quantities of Resident Registration Numbers are being stored and managed in these corporations and public institutions. These regulations are managed from Privacy Protection Law and Information Communications Network Law.

(3) Resident Registration Number Handling Law

Other than government based special demand/permission, Personal Identification Information such as Resident Registration Number's strict handling procedure was first applied through The Promoting

Usage of Information and Communication Network and Information Protection Legislation on Feb. 17, 2012 (정보통신망 이용촉진 및 정보보호 등에 관한 법률(Feb. 17 2012). Continuously, Privacy Protection Act(법률 제11990호 2013.8.6. 일부개정) prevented unnecessary collection of Resident Registration Number from every social field in Korea via on and off-line. While other Personal Identification Numbers(passport number, driver license number, alien registration number) can be modified with governments approval. However, even with governments approval, changing Resident Registration Number will be considered as an illegal act; only through legislation's specific demand and permission, RRN change can be handled legally and this is the most significant difference compared to other Personal Identification Numbers. 'Resident Registration Number handling ground's enforcement regulation' from Privacy Protection Act 14107 (법률 14107호), revised on March 29 2016 and scheduled implementation on March 30 2017 is excluded.

Ⅱ. Constitutional Court's Resident Registration Number Law Decision

1. The Background to Constitutional Court's Decision on Resident Registration Number Change

Resident Registration Number is inherently unchangeable, privately subordinated and tied to an individual for life when granted. The Resident Registration Law basically does not accept changes to the Resident Registration Number, the only case that changes can be applied is when there is an error within the Resident Registration Number and the purpose is to fix the error. Within this situation, on Dec. 23 2015, the Constitutional Court announced the case (2013헌자68, 2014헌마499) that the Article 7 of Resident Registration Number Law, not having regulations for changing individual's Resident Registration Number while issuing Resident Registration Number based on personal information, violates the individual's private information disclosure rights.

2. Resident Registration Law Article 7. Constitutional Discordance Adjudication (헌재 2015.12.23~213헌바68, 2014헌마449(병합))

(1) Event Outline

(2) The Main Summary and Format

① Subject of judgement

The majority opinion is that the applicants claim that the clauses above are not the violation of the constitution, but not having any regulations for 'Resident Registration Number change' due to false use of Resident Registration Number is the violation of constitution; which means that it is a violation of constitution not to have any regulations for changing Resident Registration Number. Therefore, the Resident Registration Number Law 제7조 was the subject to judgement, due to its most relevance of the applicants claim.

② Restricted Basic Rights

Private Information Disclosure Right is the right for an individual to decide when, where and who the individual will allow to disclose one's personal information. Personal informations that are subject to this Private Information Disclosure Right are information that helps identify personal characteristics such as: physical information, personal principles, social status and etc… Actions such as Investigation, collection, storage, handle and usage on these personal informations, principally falls in to the category of restrictions to Private Information Disclosure Right.

Resident Registration Number is a personal information that identifies an individual.

The Subject of Judgement Laws does not include regulations on the change of Resident Registration Number while it is granted, managed, used. Thus, the government is restricting applicants' Private Information Disclosure Rights by restricting the Resident Registration Number Change due to identity theft and leaked private information.

③ Constitutional Discordance Adjudication and Temporary Application Order

If the Constitutional Court makes this decision of unconstitutionality related to the subject in judgement, the Resident Registration Number system will lose its basis regulation and its absence of legality in Resident Registration Number will be inevitable. Therefore, the Constitutional Court will

sentence a constitutional discordance adjudication instead, and until the legislator legislates a improved modified system, the current Resident Registration Number system will be still in effect. The legislator must legislate a new system by Dec. 31 2017, and if not, the article subject to judgement will lose its effectiveness

(3) Constitutional Court's Decision related to Private Information Disclosure Right

The Constitutional Court announced that preventing changes of Resident Registration Number, without considering the harm that can be done due to Resident Registration Number being leaked or abused, can be an excessive violation to Private Information Disclosure Right.

When an applicant fulfilled the requirments set by the Legislators and the Resident Registration Number Change is permitted through evaluations of Government Administarions and Judicial Authority with objectivity and fairness, there would not be confusions. The majority saw not permitting the Resident Registration Number Change without considering damages caused by leaked and abused Resident Registration Number is not fulfilling minimum privacy principles and the lawful balance. Related to the Resident Registration Number Change, the Constitutional Court made a decision that Subject of Judgment Laws without containning the Resident Registration Number Change Laws violates Private Information Disclosure Rights due to violation of the principle of proportionality.

3. The Significance of Constitutional Court Decision and Legislative's Improvement Plan

The Constitutional Court make decisions for improving the convenience of the residents and national security, public order, taxation and social welfare related administrative affairs to be handled efficiently in a positive and constitutionally agreeable manner within the Resident Registration Number system; simultaneously, acknowledging the limits and problems of the current Resident Registration Number system where personal information can be leaked and abused; in the current advanced information and smart-phone/media era; furthermore, even considering the future measure of legislation, the Constitutional Court chose to protectpersonal informations to balance and harmonize the issue. Since the deadline that Constitutional Court has assigned is Dec. 31 2017, after the 20th

National Assembly Opening, through sufficient debates of Resident Registration Number Law should be revised.

Ⅲ. The Evaluation of Constitutional Court Decision.

1. Expansion Decision of Subject to Judgement Provision Relation

Judge Jin-Sung Lee's opposing opinion: "Applicants claim of legislative omission is not the Resident Registration Number system itself, but it is the grant system of the Resident Registration Number system, this matter should subject the judgement to Resident Registration Number Law system Aritle 7 Section 4" If the whole Article 7 of Resident Registration Number Law is subject to judgement, the Resident Registration Number chart system itself becomes constitutionally violated, therefore, the false omissions claim must be towards the grant system of Resident Registration Number Article 7 Section 3 and 4.

2. Allowing Resident Registration Number Change and Private Information Disclosure Right

The Constitutional Court announced on May 26 2005 99헌마513, 2004헌마190병함 Private Information Disclosure Right that an individual has a right to decide where, when and to what extend his or her private information can be used. Basic human rights based on constitutional law article 17, freedom of privacy and secrecy, human dignity and value/right to pursue happiness on article 10 line 1, the free-democracy of our constitution and citizen's sovereignty and democracy's principle will be put to consideration, and it is not possible to include Private Information Disclosure Right on Law Articles mentioned above (skip) These are considered as basic rights based on ideological principles unless certerin laws are mentioned in the Constitutional Law related to Private Information Disclosure Right.

The beginning of Article 17 states: not every citizen experience privacy violation, is a passive protection of privacy right. It is considered to be valid by the latter part of Constitutional Law Article 10: freedom of pursuing individual happiness. The Constitutional Court's position is that Resident Registration Number is an information that identifies individual's personal information, the subject to

judgement is obstructing the individual applicants from protecting Privacy Information Disclosure Right by not having regulations to change their Resident Registration Number, while granting, managing and using Resident Registration Number to the individual citizen applicants.

Judge Chang-Ho Kim and Yong-Ho Cho's opposing opinion states "allowing individuals to change their Resident Registration Number weakens the purpose of efficiently identifying individuals." From National Security point fo view, the necessity of individual citizens identification, crime concealment, tax/liability evasion and identity fraud could become abusive and difficult to manage. Furthermore, various informational change and enormous social expense due to change of Resident Registration Number system will be inevitable. Though, measures to prevent Resident Registration Number information leakage and piracy is being arranged based on Private Information Disclosure Right and Information Communications Network Act, the individuals who has already been exposed to Resident Registration Number leakage and piracy are inevitable to face the same problems without being able to change the Resident Registration Number. Therefore, for more fundamental protection for personal informations, allowing to change individual's Resident Registration Number is the most viable solution, as the majority opinion states.

3. Allowing Resident Registration Number Change and Weakened Function of Resident Registration Number

The majority opinion is that, changing individual's Resident Registration Number by an established linked system between the old Resident Registration Number and the new Resident Registration Number, administration with fairness and subjectiveness, or even through a private administrations screening, the concern of Resident Registration Number's individual identification and confirmation functions being weakened will not cause too much of social problems, even with 1-2 years term of renewal and large quantity of applications.

However, name is a component that an individual chooses and according to Family Relation Registration Related Laws; on birth registration, it is reported to Family Relation Registration and Resident Registration Number information; in the other hand, Resident Registration Number is (mandatorily)granted by the government to the citizen by the citizen's report, these two system shows fundamental differences. Furthermore, Unlike Resident Registration Number, name could overlap between multiple individuals and name is an information of an individual that becomes meaningful

when it's combined with other personal information. Even official certificates renewals is about deciding on the time period of the certificate, the fundamental legal fact that it is for a 'specific individual's official certificate' does not change. When Official Certificate(NPKI, GPKI) is being issued for the first time, it is issued based on the applicants name and Resident Registration Number; which means even the Official Certificate system is based on Resident Registration Number system as well.

Therefore, comparing the change of name or officials certificate to Resident Registration Number and claiming there will not be any problem cannot be a valid argument. Resident Registration Number is a personal information that has its difference because of its personal uniqueness, identification. Therefore, in order to change individual's Resident Registration Number, there must be strict requirements and thorough screening based on exquisite standards and procedures

Session 1-2

일본의 개인식별번호법제 현황과 문제점

趙 元済 | 駒澤大学法学専門大学院

日本における個人識別型番号に関する一考察

駒澤大学法学専門大学院
趙　元済

目次

Ⅰ．はじめに

現在、人々の生活営為の多くは、インターネットでの情報のやり取りをはじめ、バンキングやショッピングに見られるように、パソコンやスマホ等の普及によるインターネットによって成り立っているといっても過言ではない。こうした情報化社会の進展に伴って、インターネット上の不正なアクセスを防止するために、本人確認の必要性と正確性が欠かすことができない課題となっているように、インターネット上でのセキュリティ対策は、個人のみならず、社会、あるいは国全体にとって最重要課題の１つとなっている。

ところで、日本では、個人がインターネット上で金融取引をする際に、本人確認のための認証制度や追加認証制度を採択していない。このことは、預貯金者がインターネットバンキングを行う際に、本人確認のための追加認証をすることなく、ID やパスワードおよび乱数表（あるいはワンタイムパスワード）のみで資金の振替えなどを自由に行うことができる、ということを意味する。

そして、日本では、これまで、韓国のように、各個人に番号が当てられ、当該番号が記載されている住民登録証という ID カードが存在していなかった。このため、一例として日本における銀行口座開設の際に本人確認が必要な場合に、多くの者は、運転免許証などの確認で本人確認が行われることになろう。これらを所持していない者は、写真の入っていない健康保険証などが使用されている。もちろん、以上のような本人確認の方法は、対面によるアナログ方式であって、デジタール方式のインターネット上での本人確認の方法は、2003 年から始まった住民基本台帳カードの交付とこれに書き込まれた電子証明書の発行以

降である。同住民基本台帳カード（以下「住基カード」という。）の交付は、2003年（平成15年）8月25日から、希望者に対して、住まいの市区町村という基礎的地方公共団体が交付しているものであった[1]。行政サービス、とりわけ税の確定申告においては、インターネットを通じて手続をする際に、他人によるなりすましやデータ改ざんを防ぐために用いられる本人確認の手段として、2002年施行の電子署名に係る地方公共団体の認証業務に関する法律（公的個人認証法）など[2]に基づいて、地方公共団体による公的個人認証サービスの電子証明書が2004年から開始された。たとえば、納税者は、同公的個人認証をもって、国税電子申告・納税システム（e-Tax）を利用し、所得税・法人税・消費税の確定申告等を行っており、地方税ポータルシステム（eLTAX)を利用し、法人事業税・法人県民税の申告等 を行うことができるようになった。これにより、納税者は、税務署等に出向かなくても、租税の申告などが可能となったのである。

以上の住基カードとこれによる本人確認のための電子証明書は、2015年12月22日をもって終了し、現在における本人確認は、2013年施行の「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「個人番号法」という。）が2015年9月に改正されており、現在では、住基カードに代わって個人に番号が当てられた個人番号（マイナンバー）の通知と、個人番号カードの交付および同交付に伴う電子証明書の発行によって行われることになっている。つまり、現在、日本では、2015年 10月から、以上の住基カードに代わって、個人に番号が当てられた個人番号が通知されており、翌年 1月からの本人の申請による個人番号カードの交付が開始されている。同個人番号法は、番号利用法、あるいはマイナンバー法と呼ばれており、2015年10月から始まっている「個人番号制」の根拠となる法律である。また、同個人番号カードは、2002 年施行の電子署名に係る地方公共団体の認証業務に関する法律が改正されることによって、電子証明書の種類としてインターネット上のログイン手段として用いられることになった。

ところで、日本の個人番号制は、本人の申請という任意による個人番号カードの取得とその利用である。この点において、日本の個人番号カードは、強制的に取得させられる韓国の住民登録証と異なるものである。個人番号カードを取得していない者は、インターネ

---

[1] 住基カードの交付状況を見てみると、2015年3月31日現在、累計枚数が約920万枚（有効交付枚数710万枚）である（これについては、 同住民基本台帳カード総合情報サイト；http://juki-card.com/about/index.html 参照)。

[2] 申請・届出などの行政手続におけるオンラインの整備を図る法律としては、電子署名に係る地方公共団体の認証業務に関する法律（公的個人認証法）のほかに、行政手続等における情報通信の技術の利用に関する法律（行政手続オンライン化法） および行政手続等における情報通信の技術の利用に関する法律の施行に伴う関連法律の整備等に関する法律（整備法）がある。これら3つの法律をまとめて「行政手続オンライン化関係三法」と称されている。

ット上での公的認証による本人確認を行うことができず、インターネット上での行政手続を行うことができないのみで、従来通りのインターネットショッピングやバンキング等を行うことになる。つまり、国民がインターネットを通じて、行政に対する手続として申請や届け出を行おうとする場合には、個人番号カードの取得が前提条件となる。このように、個人番号カードの取得が任意であるが故に、限定的なものとして少数に留まることになるとすれば、行政手続のオンライン化における国民の利便性の向上も、一部的かつ限定的な効果しかないと考えられよう。これに対して、個人番号はすべての国民に付与されているため、行政の方からすれば、税の確定や給付などの行政事務の遂行における効率化と公平さを確保することになるという大きなメリットをもたらすことになるものの、個人番号による特定個人情報ファイル[3]の検索・管理に対しては、プライバシーないし個人情報保護との観点からその適正な運用が問われることになろう。

拙稿告では、以上の問題認識の下で、個人番号制の前身である住民基本台帳カードおよび 住民基本台帳のネットワークシステムについての意義などを一瞥し、現在、採択されている個人番号制の意義および問題点などについて見てみる。

Ⅱ．住民基本台帳法と住民基本台帳のネットワーク化

１．　住民基本台帳カードとこれによる電子証明書の発行

住民基本台帳法（以下「住基法」という。）は、住民登録法を廃止し、同法に代わって 1967 年（昭和 42）に制定されたものである。そして、1999 年の住基法の改正により、市区町村の住民基本台帳に記録されている者（＝日本国民）に 11 桁の住民票コードを割り当てること、いわゆる 住民基本台帳カード（以下「住基カード」という。）を交付するとともに、行政機関等に対する本人確認情報を提供し、市町村の区域を越えた住民基本台帳に関する事務の処理を行うため、地方公共団体共同のシステムとして、各市町村の住民基本台帳のネットワークシステム（以下「住基ネット」という。）が構築された。住基ネットは、地方公共団体と行政機関で個々の日本国民を特定する情報を共有・利用することを目的として構築され、稼働したシステムである。

住基カードの交付は、2003 年 8 月 25 日に開始された。翌年からは、同カードに電子証明書が書き込まれることになり、これによるネット上での本人確認の手段として公的個人認証サービスの電子証明書制度が開始された。これにより、納税者は、税務署等に出向かうことなくとも、租税の申告などが可能となったのである。その後、2010 年から、コンビニエンスストアなどに置いている端末による住民票の写し・印鑑登録証明書の交付サービ

[3] 「特定個人情報」とは、個人番号をその内容に含む個人情報をいい（番号法 2 条 8 項)、「特定個人情報ファイル」とは、個人番号をその内容に含む個人情報ファイルをいう（同条 9 項)。

スが東京都渋谷区、三鷹市、千葉県市川市で開始された。

以上は、国民の便宜を図るための制度改善である。ところが、住基ネットに関しては、市区町村の住民基本台帳に記録されている者（＝日本国民）に11桁の住民票コードが割り当てられていることから、プライバシーの保護に反することや個人情報保護法に反するなどの違法性や、セキュリティに対する不安から、同住基ネットに参加接続しない地方公共団体をはじめ、反対運動も各地で起きた。住基ネットをめぐっては、人格権やプライバシー権などの侵害を理由とする差止め請求や損害賠償請求訴訟が全国各地で60件近く提起されていた[4]。ところが、以下の最高裁判所平成２０年（2008年）３月６日損害賠償請求事件の判決により、全国各地で提起された住基ネットの違法性をめぐる裁判は、収束に向かうことになった[5]。

その後、かつて接続していなかった地方公共団体も順次接続し、2015年（平成27年）3月30日に福島県矢祭町が接続したのを最後に全地方公共団体の接続が完了した。

２．住基ネットをめぐる裁判

これをめぐっては、最高裁判所平成２０年（2008年）３月６日損害賠償請求事件の判決が参照となる。本件の事実概要は以下の通りである。住民らは、行政機関が住基ネットにより住民らの個人情報を収集、管理又は利用（以下、併せて「管理、利用等」という。）することについて、これらが憲法１３条の保障する住民らのプライバシー権その他の人格権を違法に侵害するものであるなどと主張して、住民らの住民基本台帳を保管する各市に対し、人格権、公権力から監視されない権利等が侵害され、精神的損害を被ったと主張し、原告らが居住する被告各市に対し、損害賠償を求めた事案である。

第１審である大阪地方裁判所平成１６年（2004年）２月２７日損害賠償請求事件の判決によれば、住民票コード自体は、無作為に作成された数字であるから、住民票コードの数字そのものからは、氏名、住所、男女の別、生年月日等の個人情報が推知されるものではない等、原告らが、住民票コードを割り振られたことにより、原告らの人格権、あるいは何らかの人格的利益が侵害されたとは認められないとされ、原告の請求は棄却された。

控訴人Ａら４名が、住民基本台帳からの住民票コードの削除等の請求を追加した大阪高等裁判所平成１８年（2006年）１１月３０日損害賠償請求控訴事件においては、住基ネット制度には、個人情報保護対策の点で無視できない欠陥があるといわざるを得ず、住民個々人の多くのプライバシー情報が、本人の予期しない時に予期しない範囲で行政機関に保有され、利用される危険が相当あるものと認め、行政目的実現手段として合理性を有しないものといわざるを得ず、控訴人らの人格的自律を著しく脅かすものであり、プライバシー

[4] 三宅弘「個人情報の保護と個人の保護」ジュリスト1422号（2011年）79頁参照。

[5] 篠原俊博「住民基本台帳制度の歴史的意義と今日的意義」地方自治５月号（2015年）９頁。

権を著しく侵害するとし、控訴を一部認容した判決が下された[6]。

[6] 同控訴事件の判決は、「住基ネットの対象となる本人確認情報は、「氏名」「生年月日」「男女の別」及び「住所」の４情報に、「住民票コード」及び「変更情報」を加えた６情報である。一般的には秘匿の必要性の高くない４情報や数字の羅列にすぎない住民票コードについても、その取扱い方によっては、情報主体たる個人の合理的期待に反してその私生活上の自由を脅かす危険を生ずることがあるから、本人確認情報は、いずれもプライバシーに係る情報として、法的保護の対象となり（最高裁判所平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁参照)、自己情報コントロール権の対象となるというべきである。…（省略）…もっとも、プライバシーに係る情報の中にも、思想、信条等の人格的自律に直接関わるような秘匿の必要性の高い情報（固有情報）もあれば、そこまでの秘匿の必要はない情報（外延情報）もあることは上述のとおりであり、それらの保護の必要性が一様のものであるとは考え難い。特に、本人確認情報は、公権力との関係でみれば、他の地方公共団体や行政機関において行政目的実現のために必要な範囲で個人識別情報として収集、保有、利用等する必要のある場合があることはいうまでもないことである（住基法１条もそれを予定している。)。このような個人識別情報としての本人確認情報の性質を考慮すれば、その収集、保有、利用等については、〔１〕それを行う正当な行政目的があり、それらが当該行政目的実現のために必要であり、かつ、〔２〕その実現手段として合理的なものである場合には、本人確認情報の性質に基づく自己情報コントロール権の内在的制約により（もしくは、公共の福祉による制約により)、原則として自己情報コントロール権を侵害するものではないと解するのが相当である。しかし、本人確認情報の漏えいや目的外利用などによる、住民のプライバシーないし私生活上の平穏が侵害される具体的危険がある場合には、上記〔２〕の実現手段として合理性がないものとして、自己情報コントロール権を侵害することになり、住基ネットによる当該本人確認情報の利用の差止めをすべき場合も生じるものと解される。」という一般論を述べながら、住基ネットによる本人確認情報漏えいの危険性の有無について検討を行い、現時点において、住基ネットのセキュリティが不備で、本人確認情報に不当にアクセスされたりして、同情報が漏えいする具体的危険があるとまで認めることはできないと判断し、住基ネットによるデータマッチング等の危険性の有無については、住基ネットの運用によって控訴人らが主張するようなデータマッチングや名寄せが行われることは考え難いといえなくもないとしており、「住基ネット制度には個人情報保護対策の点で無視できない欠陥があるといわざるを得ず、行政機関において、住民個々人の個人情報が住民票コードを付されて集積され、それがデータマッチングや名寄せされ、住民個々人の多くのプライバシー情報が、本人の予期しない時に予期しない範囲で行政機関に保有され、利用される危険が相当あるものと認められる。そして、その危険を生じさせている原因は、主として住基ネット制度自体の欠陥にあるものということができ、そうである以上、上記の危険は、抽象的な域を超えて具体的な域に達しているものと評価することができ、住民がそのような事態が生ずる具体的な危険があるとの懸念を抱くことも無理もない状況が生じているというべきである。したがって、住基ネットは、その行政目的実現手段として合理性を有しないものといわざるを得ず、その運用に同意しない控訴人らに対して住基ネットの運用をすることは、その控訴人らの人格的自律を著しく脅かすものであり、住基ネットの行政目的の正当性やその必要性が認められることを考慮しても、控訴人らのプライバシー権（自己情報コントロール権）を著しく侵害するものというべきである。」と判示している。

ところが、最高裁は、上告人敗訴部分を破棄し、被上告人ら（原告）の控訴をいずれも棄却する判決を下した。すなわち、最高裁判決によれば、行政機関が住基ネットにより住民である被上告人らの本人確認情報を管理、利用等する行為は、個人に関する情報をみだりに第三者に開示又は公表するものということはできず、当該個人がこれに同意していないとしても、憲法１３条により保障された上記自由を侵害するものではないと解するのが相当であるとされたのである。

Ⅲ．個人番号制度

１．個人番号について

個人番号とは、個人番号法の成立によるものであり、住民票コード（住民基本台帳法（昭和四十二年法律第八十一号）第七条第十三号に規定する住民票コードをいう。以下同じ。）を変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう（番号法 2 条 5 項）。つまり、個人番号は、国民一人ひとりが持つ 12 桁の番号のことである。2015 年 10 月から、住民票を有する全ての人に、1 人 1 つの個人番号が通知されている。外国籍でも住民票のある方も、その対象となっている。永住者、高度専門職第 2 号[7]および特別永住者には、日本人と同様に扱われることになっている。

1999 年の住基法の改正による住基カードと住民基本台帳のネットワーク化に対しては、前記に見るように、反対運動も各地で起き、また同ネットワークを差し止めるための裁判が起こされたが、個人番号制度に関しては、反対論がそれほど盛り上がっているようにみえないとして、こうした世論の意外な反応の理由については、より公平・公正な社会を築くための社会的基盤であり、社会保障がきめ細やかにかつ的確に行われるために必要な制度であるという立法趣旨が国民に浸透していること、また、住基ネット導入時の教訓を踏まえて、個人保護対策に相当に力を入れた仕組みとなっていること、そして「個人番号」の通称や「マイナチャン」というキャラクターなどのソフトなイメージ戦略も奏功していること、最後に住基ネットに係る事務は地方公共団体の自治事務であったが、個人番号制

[7] 高度専門職第 2 号とは、日本の学術研究や経済の発展に寄与することが見込まれる高度の専門的な能力を持つ外国人の受入れをより一層促進するため、在留期限 5 年の「高度専門職 1 号」又は高度人材外国人としての「特定活動」の在留資格をもって一定期間在留した者を対象に、在留期限を無期限とし、活動制限を大きく緩和した在留資格として設けられたものをいう。

度に係る事務は法定受託事務[8]とされていることも地方公共団体からの反乱を抑止しているといようなことが挙げられている[9]。

２．個人番号指定と通知

個人番号に関しては、市町村長の仕事となっている。市町村長は、個人番号法第７条第１項又は第２項の規定により個人番号を指定するときは、あらかじめ地方公共団体情報システム機構（以下「機構」という。）に対し、当該指定しようとする者に係る住民票に記載された住民票コードを通知するとともに、個人番号とすべき番号の生成を求めるものとする（法８条１項）。機構は、前項の規定により市町村長から個人番号とすべき番号の生成を求められたときは、政令で定めるところにより、次項の規定により設置される電子情報処理組織を使用して、以下に掲げる要件に該当する番号を生成し、速やかに、当該市町村長に対し、通知するものとする（同条２項）。その要件とは、①　他のいずれの個人番号（前条第二項の従前の個人番号を含む。）とも異なること、②　前項の住民票コードを変換して得られるものであること、③　前号の住民票コードを復元することのできる規則性を備えるものでないこととなっている。そして、以上の機構は、前項の規定により個人番号とすべき番号を生成し、並びに当該番号の生成及び市町村長に対する通知について管理するための電子情報処理組織を設置するものとなっている（同条３項）。

個人番号法７条により、市町村長（特別区の区長を含む。以下同じ。）は、住民基本台帳法第三十条の三第二項の規定により住民票に住民票コードを記載したときは、政令で定めるところにより、速やかに、次条第二項の規定により機構から通知された個人番号とすべき番号をその者の個人番号として指定し、その者に対し、当該個人番号を通知カード（氏名、住所、生年月日、性別、個人番号その他総務省令で定める事項が記載されたカードをいう。以下同じ。）により通知しなければならない（法７条１項）。市町村長は、当該市町村（特別区を含む。以下同じ。）が備える住民基本台帳に記録されている者の個人番号が漏えいして不正に用いられるおそれがあると認められるときは、政令で定めるところにより、その者の請求又は職権により、その者の従前の個人番号に代えて、次条第二項の規定により機構から通知された個人番号とすべき番号をその者の個人番号として指定し、速やかに、

---

[8] 地方自治法２条８項の規定から、地方公共団体の事務には、①地域における事務、いわゆる自治事務と、②法定受託事務の二つの種類となる。法定受託事務については、同法２条９項および10項がこれを定めている。地方自治法１４条により、地方公共団体は、法令に違反しない限りにおいて地方自治法２条２項の事務に関し、条例を制定することができると定めている。この点においては、法定受託事務とは、法解釈上、自治事務と異なるものとして扱われる必要がないものといえよう。ところが、実定法の多くの規定（地方自治法 245 条の７に定める「是正の指示」および同条の８に定める「代執行等」）にみられるように、法定受託事務の処理の際には、自治事務の処理とは明らかに異なる国等の関与の手法が定められている。

[9] 人見剛「番号法における個人番号制度をめぐる問題」法律時報 88 巻４号（2016 年）１頁。

その者に対し、当該個人番号を通知カードにより通知しなければならない（同条2項）。

３．個人番号カード

2016年（平成28年）1月から、本人の申請による個人番号カードの交付が開始されている。個人番号カードは、個人番号を証明する書類や本人確認の際の公的な身分証明書として利用でき、また、様々な行政サービスを受けることができるようになるICカードのことをいう。交付手数料は、当面の間無料である（本人の責による再発行の場合を除く）。表面には、氏名、住所、生年月日、性別、顔写真、電子証明書の有効期限の記載欄、セキュリティコード、サインパネル領域（券面の情報に修正が生じた場合、その新しい情報を記載（引越した際の新住所など））、臓器提供意思表示欄が記載され、個人番号は裏面に記載されている。

個人番号カードは、金融機関等本人確認の必要な窓口で身分証明書として利用できるが、個人番号をコピー・保管できる事業者は、行政機関や雇用主等、法令に規定された者に限定されているため、規定されていない事業者の窓口において、個人番号が記載されているカードの裏面をコピー・保管することはできない。

個人番号カードの交付等に関する法制について見てみると、市町村長は、政令で定めるところにより、当該市町村が備える住民基本台帳に記録されている者に対し、その者の申請により、その者に係る個人番号カードを交付するものとする。この場合において、当該市町村長は、その者から通知カードの返納及び前条の主務省令で定める書類の提示を受け、又は同条の政令で定める措置をとらなければならない（法17条1項）。個人番号カードの交付を受けている者は、住民基本台帳法第二十四条の二第一項に規定する最初の転入届をする場合には、当該最初の転入届と同時に、当該個人番号カードを市町村長に提出しなければならない（同条 2 項）。前項の規定により個人番号カードの提出を受けた市町村長は、当該個人番号カードについて、カード記録事項の変更その他当該個人番号カードの適切な利用を確保するために必要な措置を講じ、これを返還しなければならない（同条3項）。第二項の場合を除くほか、個人番号カードの交付を受けている者は、カード記録事項に変更があったときは、その変更があった日から十四日以内に、その旨を住所地市町村長に届け出るとともに、当該個人番号カードを提出しなければならない。この場合においては、前項の規定を準用する（同条4項）。個人番号カードの交付を受けている者は、当該個人番号カードを紛失したときは、直ちに、その旨を住所地市町村長に届け出なければならない（同条5項）。 個人番号カードは、その有効期間が満了した場合その他政令で定める場合には、その効力を失う（同条6項）。個人番号カードの交付を受けている者は、当該個人番号カードの有効期間が満了した場合その他政令で定める場合には、政令で定めるところにより、当該個人番号カードを住所地市町村長に返納しなければならない（同条7項）。前各項に定めるもののほか、個人番号カードの様式、個人番号カードの有効期間及び個人番号カード

の再交付を受けようとする場合における手続その他個人番号カードに関し必要な事項は、総務省令で定める（同条８項）。

４．　公的個人認証サービスの電子証明書

公的個人認証サービスの電子証明書は、市区町村窓口で発行した際、個人番号カード（IC カード）の中に記録して渡されることになる。電子証明書は、個人番号カードの中に格納されるので、既に個人番号カードを取得されている方は持参し、まだ個人番号カードを取得されていない方は、個人番号カードの取得が先となる。多くの市区町村では、同じ窓口で個人番号カードと電子証明書の発行を行っている。同証明書は、法律に基づき「地方公共団体情報システム機構」が運営しているシステムであり、信頼性の高い電子証明書を利用者の方々に提供することで、国や地方公共団体が提供しているオンライン申請を安全に行うためのものである。つまり、国民は、公的個人認証サービスで発行された電子証明書を利用して、行政機関等が提供しているインターネットを利用した電子申請や届出サービスなどを利用することができる。同利用のためには、電子証明書の発行はもちろんのこと、IC カードリーダライタが必要である。同 IC カードリーダライタとは、IC カードに記録された電子情報を読むための機器である。このように、公的個人認証サービスを利用したオンラインによる行政手続きを行なうためには、電子申請などに利用するインターネットに接続されたパソコンと、パソコンで電子証明書を利用するために必要となる IC カードリーダライタの準備が必要である。

個人番号カードの利用におけるセキュリティーに関しては、アクセス権の制御が行われており、IC チップ内の各アプリケーション間は「アプリケーションファイアウォール」により独立しており、アプリケーションごとに条件や暗証番号等のアクセス権情報を設定することにより、各サービス用システムから異なるアプリケーションへのアクセスを制御している。アプリケーション毎に異なる暗証番号を設定して情報を保護し、また暗証番号の入力を一定回数以上間違えるとカードがロックされる仕組みとなっている。そして、セキュリティーとして、耐タンパー性（tamper resistance）[10]が挙げられている。個人番号カードの IC チップは、こうした偽造目的の不正行為に対する耐タンパー性を有しており、高いセキュリティ性を確保していると説明されている。

５．個人番号カードと住基カードとの違いについて

1999 年の住民基本台帳法（以下「住基法」という。）の改正と、その後、2003 年 8 月 25 日に開始された住民基本台帳カードの交付、その翌年からの同カードに書き込まれた電子

[10]　耐タンパー性とは、IC チップ内の情報が不正に読み出されたり、解析されようとした場合、自動的に内容が消去される等の対抗措置が講じられる性質のことである。

証明書と、現在の個人番号カードとの間には、以下のような違いがある[11]。

住民基本台帳カードとマイナンバーカードの比較

	住民基本台帳カード	マイナンバーカード
1 券面の記載内容	○住民票コードの券面記載なし ○顔写真は選択制	○個人番号を券面に記載(裏面) ○顔写真を券面に記載
2 電子証明書	○署名用電子証明書(e-Taxでの確定申告等の電子申請に使用)	○署名用電子証明書 ○利用者証明用電子証明書(新規)(コンビニ交付やマイナポータルのログイン等、本人であることの認証手段として使用) ○民間利用可能
3 手数料(電子証明書)	500円が主 (電子証明書を掲載した場合は1,000円)	無料(電子証明書含む)
4 有効期間	○発行日から10年 ※電子証明書(署名用)は3年	○発行日から申請者の10回目の誕生日まで (ただし、20歳未満の者は容姿の変化が大きいため、申請者の5回目の誕生日まで) ※電子証明書(署名用・利用者証明用)は発行日から5回目の誕生日まで
5 利便性	○身分証明書としての利用が中心 ○市町村による付加サービスの利用(コンビニ交付、図書館利用等)	○身分証明書としての利用 ○個人番号を確認する場面での利用(就職、転職、出産育児、病気、年金受給、災害等) ○市町村、都道府県、行政機関等による付加サービスの利用 (図書館利用等の他、健康保険証、国家公務員身分証等) ○コンビニ交付利用の拡大(利用者証明用電子証明書の活用による) ○電子証明書による民間部門を含めた電子申請・取引等における利用

Ⅳ. 個人情報保護と個人番号の利用

1. 個人情報保護法制度について

個人情報の保護に関する法律[12]は、個人識別符号が含まれるものをも個人情報として保護の対象とした。従来、個人情報保護法２条１項により、「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。）と定義されていた。ところが、改正個人情報法２条１項は「個人情報」について、生存する個人に関する情報であって、① 当

---

[11] これは、総務省のホームページ；総務省トップ >政策 >地方行財政 >個人番号制度と個人番号カード > 個人番号カード（http://www.soumu.go.jp/kojinbango_card/03.html）。

[12] 個人情報保護法は、2015 年９月９日にその改正法（平成 27 年９月９日法律第 65 号）が公布され、2016 年１月１日にその一部が施行され、なお、公布日から起算して２年を超えない範囲内において政令で定める日に全面施行されることとなっている。同個人情報保護法は、2015 年９月９日に個人情報の保護に関する法律および個人番号法の一部を改正する法律案が成立し、公布されたことによるものである。

該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第２号において同じ。）で作られる記録をいう。第 18 条第２項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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。）、② 個人識別符号が含まれるものと定義し、これらを保護の対象としている。

そして、「個人識別符号」については、 同法 2 条 2 項が次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものと定義している。その各号には、① 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの、② 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるものが列挙されている。

以上の個人情報保護法 2 条 2 項 1 号にあたるものとしては、指紋認識データ、顔認識データが含まれること、同項 2 号にいう個人識別符号、つまり個人に発行されるカードその他の書類に記載される番号として、旅券番号、免許証番号等が含まれており、個人識別符号となるかどうかに関する判断要素としては、一義性（個人と符合が一対一かどうか）、不変性（符号の変更が頻繁に行われないか）、本人到達性（符号に基づいて直接個人にアプローチをすることができるか）があるということが挙げられていた[13]。

以上に見るように、個人情報保護法 2 条 2 項はその 1 号および 2 号において個人識別符号について、情報単体で特定の個人を識別することができるものと定義しつつ、さらに政令でこれらを定めるとしている。同政令で定めることによって個人情報該当性を客観化することで、文字、番号、記号その他の符号といった情報が保護の対象となるか否かに関する事業者の判断が容易になるようにしたのである[14]。

そして、同法 2 条 3 項は、「要配慮個人情報」を規定している。要配慮個人情報とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報と定義されている。同要配慮個人情

[13] 座談会「個人情報保護法・個人番号法改正の意義と課題」ジュリスト 2016 年 2 月号 16 頁（No. 1489）。

[14] 日置巴美「改正個人情報保護法の概要」前掲ジュリスト 31 頁。

報 に対しては、個人情報取扱事業者は、① 法令に基づく場合、② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき、③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるときを除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない（同法 17 条 2 項）。

また、個人情報保護法 2 条 9 項は、「匿名加工情報」について、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものと定義し、次の各号としては、① 第 1 項第 1 号に該当する個人情報 当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）、② 第 1 項第 2 号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）を列挙している。

以上にみるように、個人情報保護法は、個人情報の目的外利用や個人データ（個人情報データベース等を構成する個人情報、これについては同法 2 条 6 項）の第三者提供をするためには、あらかじめ、原則的に本人の同意を得なければならない。しかし、何百万人もの個人情報を取り扱う者、いわゆる個人情報取扱事業者に、すべての者から同意を得ることを求めることは、時間的・経済的に無理な場合もあることを否めない。このことから、個人情報保護法は、個人の権益を侵害することのないようにしつつ、膨大なデータを利活用することができるように、匿名加工情報[15]に関する制度を設けたのである。つまり、個人情報保護法は、利用目的の特定や第三者提供の制限といった個人情報の取扱いに求められる義務の適用外となるよう、個人が特定できないようにデータを加工処理した「匿名加工情報」という個人情報とは別の新たなパーソナルデータの区分を設けることにしたのである。匿名加工情報の作成方法は、新設される個人情報保護委員会が、その基準を定めることになっている（同法 36 条参照）。

もちろん、個人情報保護法は、個人情報の第 3 者への提供を原則的に制限している。つまり、個人情報取扱事業者は、① 法令に基づく場合、② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき、③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき、④ 国の機関若しくは地方公共団体又はその委託を受けた者が

[15] 匿名加工情報の利活用の例としては、GPS により取得された位置情報や交通系 IC カードの乗降履歴等、物品購入の履歴、医療機関の保有する医療情報などがあり、これらの情報について、個人が特定できないようにデータを加工処理した「匿名加工情報」とし、同情報を都市開発や商品開発に複数の業者間の分野横断的な利用をすることが考えられよう。

法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるときを除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない（同法 23 条 1 項）。

ちなみに、個人情報保護法第 4 章第 1 節には個人情報取扱事業者の義務が、第 2 節には匿名加工情報取扱事業者等の義務が定められている。同委員会の個人情報取扱事業者又は匿名加工情報取扱事業者に対する監督権限などについては、個人情報保護法第 4 章第 3 節における 40 条ないし 42 条がこれを定めている。同章 4 節には民間団体による個人情報の保護の推進が定められている。個人情報保護委員会の構成ないし組織などに関しては、個人情報保護法第 5 章がこれらを定めている。同委員会は、個人情報の扱いを監視監督する権限を有する第 3 者機関である。

２．個人番号利用のための法制

さて、個人番号の利用に関しては、個人番号法 9 条が個人番号利用のための根拠規定である。個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）の全部又は一部の委託を受けた者は、当該個人番号利用事務等の委託をした者の許諾を得た場合に限り、その全部又は一部の再委託をすることができる（同法 10 条 1 項）。

そして、同法１９条が特定個人情報の提供のための根拠規定を置いている。同規定は、異なる分野に属する情報を照合するというデータマッチングを可能とするものである。ところが、同法 19 条が「何人も、次の各号のいずれかに該当する場合を除き、特定個人情報の提供をしてはならない。」と規定し、その根拠規定が第 1 号ないし第 13 号までの個別領域を挙げながら、第 14 号（「人の生命、身体又は財産の保護のために必要がある場合において、本人の同意があり、又は本人の同意を得ることが困難であるとき」）および第 15 号（「その他これらに準ずるものとして個人情報保護委員会規則で定めるとき」）という例示列挙の形態をとっており、その利用の領域拡大が法律ではなく、個人情報保護委員会規則によって可能となっている。この点からすれば、特定個人情報個人番号の野放図な提供拡大が懸念されよう。そして、2015 年 9 月 9 日に個人情報の保護に関する法律および個人番号法の一部を改正する法律案が成立し、公布され、同法によって、個人情報保護法および個人番号法の一部の改正のほかに、地方税法、厚生年金保険法、国民年金法、国税通則法、登録免許税法、住民基本台帳法、エネルギーの使用の合理化等に関する法律、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律、遺失物法等の改正を行い、個人番号の利用を目的とする法改正が行われたのである。これらの法改正により、たとえば、源泉徴収、支払調書、雇用保険被保険者資格取得届、健康保険被保険者資格取得届、厚生年金保険被保険者資格取得届等に個人番号の利用が義務付けられている。社会保険や源泉徴収票、法定調書等の各種行政機関への提出書類には個人番号、法人番号の記載が求められるので、すべての従業員とその家族の個人番号情報を企業自ら収集し、様々な厳しい規則に従い適切に管理する

必要がある。このため、改正個人番号法は、特定個人情報の取扱いに関する監督等に関する第6章を新たに設けた。

Ⅴ．おわりに　―　個人番号制による国民の利便性と行政の効率化

総務省のホームパージ[16]によれば、すでに住基ネットの施行に関する評価として、住民の利便性の向上や行政の効率化が図られたというメリットがあげられている。

また、個人番号カードの取得者が同カードを利用することのメリットについて、総務省ホームページによる[17]と、 以下のような説明がなされている。すなわち、個人番号制度導入後は、就職、転職、出産育児、病気、年金受給、災害等、多くの場面で個人番号の提示が必要となる。その際、通知カードであれば、運転免許証や旅券等他の本人確認書類が必要となるが、個人番号カードがあれば、一枚で番号確認と本人確認が可能となる。他にも、個人番号カードを取得すると、①本人確認の際の公的な身分証明書として利用できること、②市区町村や国等が提供する様々なサービス毎に必要だった複数のカードが個人番号カードと一体化できるようになること、たとえば、地方公共団体における印鑑登録証や図書カードとしての利用可能、民間におけるポイントカード、入退者管理や身分証として利用可能、③平成29年1月から開始されるマイナポータルへのログインをはじめ、各種の行政手

---

[16] 総務省トップ > 政策 > 地方行財政 > 住民基本台帳等 > 住基ネット > 住基ネットでできるようになったことは？　> 住基ネットのメリットについて (http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/daityo/01_merit.html)。総務省によると、①　住基ネットは、高齢の方を中心に大変に役立っている。年金を受給される方は、生存の確認のために「現況届」とよばれる届出を毎年しなければならないが、住基ネットの活用により2006年10月から省略できるようになっている。全国で4､000万人の方がこのメリットを享受している。届出書に記入し、50円切手を貼ってポストに行って投函することは、大した手間ではないとの指摘もある。しかし、大変さは人によって異なる。高齢になればなおさらである。住基ネットは、このような国民負担を減らすためになくてはならないものである。住基ネットの利便性を挙げている。②　身分証明書としての住基カードの有効性については、住基カードは全国で約764万枚（平成25年6月現在)。まだまだ普及は十分ではない。しかし、さまざまな事情で運転免許を持ってない方、高齢になり運転免許証を返納した方などにとっては、住基カードは身分証明書として大変貴重な存在である。③　電子申請を利用することによって、医療費控除手続きをしやすくするという利便性を挙げている。医療費控除を毎年確定申告する方も多い。その際、申告書に領収書を貼るのに手間がかかる。住基カードに格納された公的個人認証サービスの電子証明書を使ってe-Taxによる確定申告の電子申請を行った場合には、領収書は保存しておけば良いことになっており、添付は必要ない。また、税額控除を受けることができる。

[17] 注・4参照。

続のオンライン申請に利用できるようになること、④オンラインバンキングをはじめ、各種の民間のオンライン取引に利用できるようになること、⑤コンビニなどで住民票、印鑑登録証明書などの公的な証明書を取得できるようになることといった、多くの様々なメリットを享受することができるようになるという見込みであるとの説明がなされている。

確かに、住民票の取得および銀行口座開設などの場合に、役所や銀行までに行かずに、パソコンやスマホ等を使って、これらの手続きを行うことができるという国民にとっての利便性がある。これらの利便性を活かすためには、特に高齢者社会における高齢者がインターネットの使い方になれているということが大前提となろう。

ところが、実際のところ、多くの国民は、一回の住民票や印鑑登録証の発行のために、個人番号カードの交付のための申請をすることにならないと考えられよう。だとすれば、以上の個人番号カードの取得による国民の利便性の増進とは、絵に描いた餅であって、多くの国民が同利便性を享受することにはならない[18]。換言すれば、国が個人番号を通じて、税の正確な徴収や、生活保護などの給付行政における決定の正確さを図ることができるというところに、個人番号制のメリットがある一方、個人番号の活用等に関しては、なりすましの不正利用の可能性、情報漏れの危険性、政府による住民の監視などというデメリットが考えられよう。以上のデメリットを考えると、個人番号制が「国家からの自由」という「古典的な」自由に対する「浸食」となるという大袈裟な言い方は、情報化社会という時代の流れに逆行することになろうか。

また、個人番号制は、当初、税と社会保障の一体的改革を目的として、それらの分野に限定した利用として構想され、その後、東日本大震災の経験を踏まえて災害分野が加えることになった。その後、裁判手続、刑事事件捜査での利用まで含めて法定化されている（個人番号法 19 条 12 号・9 条 5 項）。しかも、個人番号・法人番号の利用に関しては、社会保障・税・災害対策以外の分野、すなわち他の行政分野及び行政分野以外の国民の利便性の向上に資する分野における利用の可能性を考慮して行われなければならないとする個人番号法 3 条 2 項、個人番号カードの利用に関しては、行政事務以外の事務の処理において個人番号カードの活用が図られるように行われなければならないとする同法 3 条 3 項、また、情報提供ネットワークシステムに関しては、特定個人情報以外の情報の授受に情報提供ネットワークシステムの用途を拡大する可能性を考慮して行われなければならないとする同法 3 条 4 項は、個人番号の利用促進法として個人番号法の基本理念を定めているものとはいえ、これらが、個人情報保護法制（とりわけ個人情報保護法 15 条・16 条、行政機関個人情報保護法 3 条・4 条・8 条）に大きな風穴が空いてしまい、これが野放図に広がることが

[18] 個人が行政手続を行う場面は、一生でさほど多くはなく、行政手続の際の添付書類削減というメリットのために、多額の税金を投入して番号制度を導入するのは無意味であるとの指摘もある（水町雅子「やさしい番号法入門」（商事法務、2014 年）67 頁）。

大いに危惧されるという点が指摘されている[19]。同様に、個人番号法は特定個人情報の利活用を重視しており、特別法である個人番号法が基本法である個人情報保護法における保護目的を緩和し利活用を優先させるのは妥当かという質問に対して、個人番号法の立法者意思として「法案の具体的条文は決して保護を緩めているわけではなく、むしろ利用に対する制約を厳格化している面があり、また特に組織面では、第三者委員会としての個人情報保護委員会を設けその独立性を確保しており、個人の権利利益の侵害は許されないという前提は基本法・特別法に共通していると解すべきであるという立法者の見解が述べられている[20]。とくに、地方公共団体は、 ①　すでにマイナンバー利用事務とされている公営住宅（低所得者向け）の管理に加えて、特定優良賃貸住宅（中所得者向け）の管理において、個人番号の利用を可能としており、 ②　地方公共団体が条例により独自にマイナンバーを利用する場合においても、情報提供ネットワークシステムを利用した情報連携を可能とし、③　地方公共団体の要望等を踏まえ、雇用、障害者福祉等の分野において利用事務、情報連携の追加を行うこととされている[21]。こうした地方公共団体における個人番号の利用は、地方公共団体が総合行政の担い手であることから来る利用の態様であるが、これについては、地方公共団体による個人情報の集積と拡大が懸念されよう。同懸念に対しては、「課税の適正化についていえば、個々の売買について、個人番号付きで領収書を作成し、これを届け出ることを義務付けているわけではないので、事業所得の把握には限界がある。社会保障についても、所得のみならず資産まで把握しなければ、真に手を差し伸べるべき者を確定することはできないが、現行の番号制度では、資産の把握までできるわけではない。」という一定の限界があることを示す見解がある[22]。

いずれにしても、情報化社会の進展に伴う個人番号制は、現時点において行政事務の効率化を図るものとして、その必要性を否めない。だが、将来的に必ず個人番号制のさらなる利用拡大が行われることになるという前提からすれば、日本における個人番号制のスタートが「民主社会」から「監視社会」への第一歩にならないように、個人番号制の厳格な運用を統制する法制度がなにより重要であろう。

---

[19] 人見剛「番号法における個人番号制度をめぐる問題」法律時報 88 巻 4 号（2016 年）2 頁。

[20] 亘理格など「質疑応答の概要」法律時報 88 巻 1 号（2016 年）86 頁。同質疑応答とは、第 15 回行政法研究フォーラムの際に行われたものである。

[21] 内閣府大臣官房番号制度担当室「個人情報の保護に関する法律および個人番号法の一部を改正する法律案（概要）」2015 年 2 月 16 日。同資料によると、『世界最先端 IT 国家創造宣言』（２０１４年６月 24 日閣議決定）等を踏まえ、さらなる効率化・利便性の向上が見込まれる分野に ついてマイナンバーの利用範囲の拡大や制度基盤の活用を図るとともに、マイナンバー制度の主たる担い手である地方公共団 体の要望等を踏まえ、所要の整備を行うとされている。

[22] 宇賀克也「番号制度導入の意義と実務上の留意点」自治実務セミナー644 号（2016 年 2 月）3 頁。

以上、ご清聴ありがとうございました。
(2016.5.31.脱稿)

일본의 개인식별형 번호에 관한 고찰

Ⅰ. 들어가며

현재 사람들의 생활의 많은 부분은 인터넷에서 정보를 주고받는 것은 물론 은행거래나 쇼핑에서 보듯이 컴퓨터와 스마트 폰 등의 보급에 따른 인터넷에 의해 이루어지고 있다고 해도 지나치지 않다. 이러한 정보화 사회의 진전에 따라 인터넷상의 부정한 접속을 방지하기 위해 본인확인의 필요성과 정확성이 간과할 수 없는 과제가 되고 있는 것처럼, 인터넷상의 보안대책은 개인뿐만 아니라 사회 혹은 국가전체 차원에서 가장 중요한 과제 중 하나가 되고 있다.

그런데 일본에서는 개인이 인터넷상에서 금융거래를 하는 경우에 본인확인을 위한 인증제도와 추가인증 제도를 채택하지 않았다. 이것은 예저금자(預貯金者)가 인터넷뱅킹을 하는 경우에 본인확인을 위한 추가인증을 하는 일 없이, ID와 Password 및 난수표(혹은 일회성 패스워드)만으로 자금의 이체 등을 자유로이 할 수 있다는 것을 의미한다.

그리고 일본에서는 지금까지 한국처럼 각 개인에게 번호가 부여되고 당해 번호가 기재된 주민등록증이라는 ID카드가 존재하지 않았다. 이 때문에 일례로서 일본의 은행계좌 개설 시에 본인확인이 필요한 경우에 많은 사람이 운전면허증 등의 확인으로 본인확인을 하게 될 것이다. 이러한 것을 소지하지 않은 사람은 사진이 없는 건강보험증 등이 사용된다. 물론 위와 같은 본인확인의 방법은 대면에 의한 아날로그방식이고, 디지털방식인 인터넷상의 본인확인의 방법은 2003년부터 시작된 주민기본대장 카드의 교부와 이에 기록된 전자증명서의 발행 이후다. 동 주민기본대장 카드(이하, '주기카드'라 한다)의 교부는 2003년 8월 25일부터 희망자에 대해 거주하는 시구정촌(市区町村) 등 기초적 지방공공단체가 교부하고 있었다[1]. 행정서비스, 특히 세금의 확정신고에 있어서는 인터넷을 통해 절차를 밟는 경우에 타인에 의한 거짓행세나 데이터 조작을 방지하기 위해 이용되는 본인확인의 수단으로서 2002년 시행된 전자서명에 관한 지방공공단체의 인증업무에 관한 법률(공적 개인인증법) 등[2]을 근거로 지방공공단체에 의한 공적개

1) 주기카드의 교부상황을 살펴보면, 2015년 3월 31일 현재 누계매수가 약 920만매(유효교부매수 710만 매)이다(이에 대해서는 동 주민기본대장 카드 종합정보사이트 ; http://juki-card.com/about/index.html 참조).

2) 신청·신고 등의 행정절차에서 온라인의 정비를 도모하는 법률로서는, 전자서명에 관련된 지방공공단체의 인증업무에 관한 법률(공적 개인인증법) 이외에 행정절차 등에서 정보통신기술의 이용에 관한 법률(행정절차 온라인화법) 및 행정절차 등에서 정보통신기술의 이용에 관한 법률의 시행에 따른 관련법률의 정비 등에 관한 법률(정비법)이 있다. 이들 3가지 법률을 종합하여 '행정절차 온라인화 관계3법'이라 칭하고 있다.

인인증서비스의 전자증명서가 2004년부터 개시되었다. 예를 들면, 납세자는 동 공적개인인증을 통해 국세 전자신고납세시스템(e-Tax)을 이용하여 소득세·법인세·소비세의 확정신고 등을 행하고 지방세 포탈시스템(eLTAX)을 이용하여 법인사업세·법인현민(県民)세의 신고 등을 할 수 있게 되었다. 이에 따라 납세자는 세무서 등에 가지 않고도 조세의 신고 등이 가능해진 것이다.

이상의 주기카드와 이에 따른 본인확인을 위한 전자증명서는 2015년 12월 22일로써 종료되고 현재의 본인확인은 2013년 시행된 '행정절차상의 특정개인을 식별하기 위한 번호의 이용 등에 관한 법률'(이하, '개인번호법'이라 한다)이 2015년 9월에 개정되어 현재는 주기카드 대신에 개인에게 번호가 부여된 개인번호(My Number)의 통지와 개인번호 카드의 교부 및 동 교부에 따른 전자증명서의 발행을 통해 이루어지게 되어 있다. 결국 현재 일본에서는 2015년 10월부터 전술한 주기카드 대신에 개인에게 번호가 부여된 개인번호가 통지되어 이듬해 1월부터 본인신청에 의한 개인번호카드의 교부가 개시되었다. 동 개인번호법은 번호이용법 혹은 My Number법이라 불리며 2015년 10월부터 시작된 '개인번호제'의 근거가 된 법률이다. 또한 동 개인번호카드는 2002년 시행된 전자서명에 관한 지방공공단체의 인증업무에 관한 법률이 개정됨으로써 전자증명서의 종류로서 인터넷상의 로그인수단으로서 이용하게 되었다.

그런데 일본의 개인번호제는 본인의 신청이라는 임의적인 개인번호카드의 취득과 이용이다. 이 점에서 일본의 개인번호카드는 강제적으로 취득해야만 되는 한국의 주민등록증과 다르다. 개인번호카드를 취득하지 않은 사람은 인터넷상의 공적인증에 의한 본인확인을 할 수 없고 인터넷상에서 행정절차를 밟을 수 없을 뿐이고 종래와 같은 인터넷쇼핑이나 은행업무 등을 하게 된다. 결국 국민이 인터넷을 통해 행정에 대한 절차로서 신청과 신고를 하려는 경우에는 개인번호카드의 취득이 전제조건이 된다. 이처럼 개인번호카드의 취득이 임의이기 때문에 제한적인 것으로서 적은 수에 그친다고 하면 행정절차의 온라인화를 통한 국민의 편리성 향상도 일부에 그치고 제한적인 효과밖에 없을 거라고 생각된다. 이에 비해 개인번호는 모든 국민에게 부여되고 있기 때문에 행정측면에서 보면 세금의 확정과 급부 등 행정사무 수행상의 효율화와 공평성을 확보하게 되는 커다란 장점도 있지만 개인번호에 의한 특정개인정보 파일[3]의 검색·관리에 대해서는 프라이버시 내지는 개인정보보호의 관점에서 그 적정한 운용이 문제될 수 있을 것이다.

본고에서는 이러한 문제의식을 토대로 개인번호제의 전신인 주민기본대장카드 및 주민기본대장의 네트워크시스템에 대한 의의 등을 일별(一瞥)하고 현재 채택하고 있는 개인번호제의 의의

3) '특정개인정보'란 개인번호를 그 내용에 포함하는 개인정보를 말하며(번호법 2조 8항), '특정개인정보파일'이란 개인정보를 그 내용에 포함하는 개인정보파일을 가리킨다(동조 9항).

및 문제점 등에 대해 살펴본다.

Ⅱ. 주민기본대장법과 주민기본대장의 네트워크화

1. 주민기본대장카드와 이에 따른 전자증명서의 발행

주민기본대장(이하, '주기법'이라 한다)은 주민등록법을 폐지하고 동법 대신에 1967년에 제정된 것이다. 그리고 1999년의 주기법 개정에 따라 시구정촌(市区町村)의 주민기본대장에 기록되어 있는 자(=일본국민)에게 11자리의 주민표 코드를 부여하는 것, 즉 주민기본대장카드(이하, '주기카드'라고 한다)를 교부함과 동시에 행정기관 등에 대한 본인확인정보를 제공하고 시정촌(市町村)의 구역을 벗어난 주민기본대장에 관한 사무를 처리하기 위해 지방공공단체 공동의 시스템으로서 각 시정촌(市町村)의 주민기본대장의 네트워크시스템(이하, '주기네트'라고 한다)이 구축되었다. 주기네트는 지방공공단체와 행정기관에서 개개의 일본국민을 특정할 정보를 공유·이용할 것을 목적으로 하여 구축되고 가동된 시스템이다.

주기카드의 교부는 2003년 8월 25일에 개시되었다. 이듬해부터는 동 카드에 전자증명서를 입력하게 됨으로써 이에 따른 인터넷상의 본인확인을 위한 수단으로서 공적 개인인증서비스의 전자증명서제도가 개시되었다. 이에 따라 납세자는 세무서 등에 가지 않더라도 조세의 신고 등이 가능하게 되었다. 그 후 2010년부터 편의점 등에 설치되어 있는 단말기에 의한 주민표의 발급·인감등록증명서의 교부서비스가 도쿄도 시부야구(東京都渋谷区), 미타카시(三鷹市), 치바현 이치카와시(千葉県市川市)에서 개시되었다.

이상은 국민의 편의를 도모하기 위한 제도개선이다. 그런데 주기네트에 관해서는 시구정촌(市区町村)의 주민기본대장에 기록되어 있는 자(=일본국민)에게 11자리의 주민표 코드가 부여되어 있으므로 프라이버시의 보호에 반하는 것과 개인정보보호법에 반하는 등의 위법성과 보안에 대한 불안에서 동 주기네트에 참가접속하지 않은 지방공공단체를 시작으로 각지에서 반대운동도 일어났다. 주기네트에 관해서는 인격권과 프라이버시권 등의 침해를 이유로 한 금지청구와 손해배상청구소송이 전국각지에서 60건 가까이 제기되었다[4]. 하지만 이하의 최고재판소 2008년 3월 6일 손해배상청구사건의 판결을 계기로 전국각지에서 제기된 주기네트의 위법성에 관한 재판은 정리수순에 들어가게 되었다[5].

4) 三宅弘「個人情報の保護と個人の保護」ジュリスト1422号(2011年) 79頁参照

그 후 그때까지 접속하지 않았던 지방공공단체도 순차적으로 접속하여 2015년 3월 30일에 후쿠시마현 야마쯔리마치(福島県矢祭町)가 접속한 것을 마지막으로 전국지방공공단체의 접속이 완료되었다.

2. 주기네트에 관련된 재판

이에 관해서는 최고법원 2008년 3월 6일 손해배상사건의 판결이 참조가 될 것이다. 본건의 사실개요는 다음과 같다. 주민들은 행정기관이 주기네트에 따라 주민들의 개인정보를 수집, 관리 또는 이용(이하, 함께 '관리, 이용 등'이라 한다)하는 것에 대해서, 이것이 헌법 13조에서 보장하는 프라이버시권 기타 인격권을 위법하게 침해하는 것이라는 등의 주장을 펴고, 주민들의 주민기본대장을 보관하는 각 시(市)에 대해 인격권, 공권력에 감시당하지 않을 권리 등이 침해되어 정신적 손해를 입었다고 주장하여 원고들이 거주하는 피고 각 시(市)에 대해 손해배상을 요구한 사안이다.

제1심인 오사카 지방법원 2004년 2월 27일 손해배상청구사건의 판결에 따르면, 주민표 코드 자체는 무작위로 작성된 숫자이므로 주민표 코드의 숫자 자체에서는 성명, 주소, 성별, 생년월일 등의 개인정보를 짐작할 수 없는 등, 원고들이 주민표 코드를 부여받음으로써 원고들의 인격권 혹은 어떠한 인격적 이익이 침해되었다고는 인정할 수 없다고 하여 원고의 청구가 기각되었다.

항소인 A등 4명이 주민기본대장에서 주민표 코드의 삭제 등의 청구를 추가한 오사카 고등법원 2006년 11월 30일 손해배상청구 항소사건에서는, 주기네트제도에는 개인정보보호대책의 관점에서 무시할 수 없는 결함이 있다고 말하지 않을 수 없고, 주민 개개인의 많은 프라이버시 정보가 본인이 예기치 않은 때에 예기치 않은 범위에서 행정기관에 보유되고 이용될 위험이 상당하다고 인정되어 행정목적의 실현수단으로서 합리성이 없는 것이라고 말하지 않을 수 없으며, 항소인들의 인격적 자율을 현저하게 위협하는 것으로서 프라이버시권을 현저하게 침해한다고 보아 항소를 일부 인용한 판결이 내려졌다[6].

---

5) 篠原俊博「住民基本台帳制度の歴史的意義と今日的意義」地方自治5月号(2015年) 9頁

6) 동 항소사건의 판결은 "주기네트의 대상이 될 본인확인정보는 '성명' '생년월일' '성별' 및 '주소'의 4정보에 '주민표 코드' 및 '변경정보'를 추가한 6정보이다. 일반적으로는 은닉의 필요성이 높지 않은 4정보와 숫자의 나열에 불과한 주민표 코드에 대해서도, 그 취급형태에 따라서는 정보주체인 개인의 합리적 기대에 반하여 그 사생활상의 자유를 위협하는 위험을 일으키는 일이 있으므로 본인확인정보는 모두 프라이버시에 관한 정보로서 법적보호의 대상이 되고(최고법원 2003년 9월 12일 제2소법정판결·민집57권8호973쪽 참조) 자기정보통제권의 대상이 되어야 마땅하다. …(생략)… 그런데 프라이버시에 관한 정보 중에도 사상, 신조 등의 인격적 자율에 직접 연관되는 것과 같은 은닉필요성이 높은 정보(고유정보)도 있고, 그 정도로 은닉할 필요성은 없는 정보(외연정보)도 있는 것은 전술한 바와 같으며, 그 보호필요성이 똑같다고

그런데 최고법원은 상고인 패소부분을 파기하고 피상고인들(원고)의 항소를 모두 기각하는 판결을 내렸다. 즉, 최고법원 판결에 따르면, 행정기관이 주기네트에 의해 주민인 피상고인들의 본인확인정보를 관리, 이용 등을 하는 행위는 개인에 관한 정보를 함부로 제3자에게 공시 또는 공표하는 것이라고는 할 수 없고, 당해 개인이 이에 동의하지 않더라도 헌법 13조에 의해 보장된 상기 자유를 침해하는 것은 아니라고 해석하는 것이 상당하다고 본 것이다.

Ⅲ. 개인번호제도

1. 개인번호에 대하여

개인번호란 개인번호법의 성립에 따른 것으로서 주민표 코드(주민기본대장법(1967년 법률 제81호) 제7조 제13호에 규정하는 주민표 코드를 말한다. 이하, 동일)를 변환시켜 얻을 수 있는 번호로서, 당해 주민표 코드가 기재된 주민표에 관련된 자를 식별하기 위해 지정되는 것을 가리킨다(번호법 2조 5항). 결국, 개인번호는 국민 개개인이 가지는 12자리의 번호이다. 2015

는 생각하기 어렵다. 특히, 본인확인정보는 공권력과의 관계에서 보면, 다른 지방공공단체나 행정기관에서 행정목적 실현을 위해 필요한 범위에서 개인 식별정보로서 수집, 보유, 이용 등을 할 필요가 있는 경우가 있다는 것은 두말할 필요 없는 일이다(주기법 1조도 그것을 예정하고 있다). 이러한 개인 식별정보로서의 본인확인정보의 성질을 고려하면, 그 수집, 보유, 이용 등에 대해서는 [1] 그것을 행할 정당한 행정목적이 있고 그것들이 당해 행정목적 실현을 위해 필요하며, 또한 [2] 그 실현수단으로서 합리적인 것인 경우에는 본인확인정보의 성질에 기초한 자기정보통제권의 내재적 제약에 따라 (혹은 공공의 복지에 의한 제약에 따라) 원칙적으로 자기정보통제권을 침해하는 것은 아니라고 해석하는 것이 상당하다. 그러나 본인확인정보의 유출이나 목적 외 이용 등에 의한 주민의 프라이버시 내지 사생활상의 평온이 침해될 구체적인 위험이 있는 경우에는, 상기 [2]의 실현수단으로서 합리성이 없는 것으로서 자기정보통제권을 침해하는 것이 되어 주기네트에 의한 당해 본인확인정보 이용을 금지해야 하는 경우도 생긴다고 해석된다."고 하는 일반론을 얘기하면서, 주기네트에 의한 본인확인정보유출의 위험성 유무에 대해 검토를 하고, 현 시점에서 주기네트의 보안대책이 불충분하며 본인확인정보에 부당하게 액세스되거나 하여 동 정보가 유출될 위험이 있다고까지 인정할 수는 없다고 판단하고, 주기네트에 의한 데이터 조합(matching) 등의 위험성 유무에 대해서는, 주기네트의 운용에 의해 항소인들이 주장하는 바와 같은 데이터 조합(matching)이나 이름식별이 이루어지는 것이 생각하기 어렵다고 말할 수도 없다고 보고, "주기네트제도에는 개인정보보호대책이라는 점에서 무시할 수 없는 결함이 있다고 말하지 않을 수 없으며, 행정기관에서 주민 개개인의 개인정보가 주민표 코드를 부착하여 집적되고 그것이 데이터 조합(matching)이나 이름식별이 되어 주민 개개인의 많은 프라이버시정보가 본인이 예기치 않은 때에 예기치 않은 범위에서 행정기관에 보유되고 이용될 위험이 상당히 있다고 인정된다. 그리고 그 위험을 발생시키고 있는 원인은 주로 주기네트제도 자체의 결함에 있다고 할 수 있고, 그런 이상, 상기 위험은 추상적인 자기영역을 넘어 구체적인 자기영역에 이르고 있다고 평가할 수 있고, 주민이 그러한 사태가 발생할 구체적인 위험이 있다고 하는 우려를 하는 것도 무리가 아닌 상황이 발생하고 있다고 해야 한다. 그러므로 주기네트는 그 행정목적 실현수단으로서 합리성이 없다고 말하지 않을 수 없고, 그 운용에 동의하지 않는 항소인들에 대해 주기네트를 운용하는 것은 그 항소인들의 인격적 자율을 현저하게 위협하는 것이며, 주기네트의 행정목적의 정당성이나 그 필요성이 인정되는 것을 고려해도, 항소인들의 프라이버시권(자기정보통제권)을 현저하게 침해하는 것이라고 해야 마땅하다." 고 판시하고 있다.

년 10월부터 주민표가 있는 모든 사람에게 한 사람 한 사람의 개인번호가 통지되어 있다. 외국 국적이라도 주민표가 있는 사람은 그 대상이 되어 있다. 영주권자, 고도전문직 제2호[7] 및 특별영주권자에게는 일본인과 마찬가지로 취급되도록 하고 있다.

1999년의 주기법 개정에 따른 주기카드와 주민기본대장의 네트워크화에 대해서는 앞에서 본 것처럼, 각지에서 반대운동도 일어나고 또한 동 네트워크를 금지청구하기 위한 소송이 제기되었지만, 개인번호제도에 관해서는 반대론이 그다지 들끓은 것으로는 보이지 않는다고 보고, 이렇듯 여론의 반응이 의외인 이유에 대해서는 보다 공평·공정한 사회를 만들기 위한 사회적 기반이고 사회보장이 촘촘하고 적확하게 이루어지는데 필요한 제도라는 입법취지가 국민에게 침투되고 있는 점, 또한 주기네트 도입 당시의 교훈을 참고하여 개인보호대책에 상당히 역점을 둔 구조가 되어 있다는 점, 그리고 '개인번호'의 통칭과 '마이나짱'이라는 캐릭터 등의 부드러운 이미지 전략도 주효하였다는 점, 마지막으로 주기네트에 관련된 사무는 지방공공단체의 자치사무였으나 개인번호제도에 관련된 사무는 법정수탁사무[8]로 되어 있다는 점도 지방공공단체로부터의 반발을 억제하고 있다는 측면이 제시되고 있다[9].

2. 개인번호 지정과 통지

개인번호에 관해서는 시정촌(市町村)의 장의 업무로 되어 있다. 시정촌(市町村)의 장(長)이 개인번호법 제7조 제1항 또는 제2항의 규정에 따라 개인번호를 지정하는 때는 미리 지방공공단체 정보시스템기구(이하 '기구'라 한다)에 대해, 당해 지정하고자 하는 자에 관련된 주민표에 기재된 주민표 코드를 통지함과 아울러 개인번호로 할 번호의 생성을 요구하도록 한다(법 8조 1항). 기구는 전항의 규정에 따라 시정촌(市町村)의 장으로부터 개인번호로 할 번호의 생성을 요구받은 때는 정령에서 정하는 바에 따라 다음 항의 규정에 따라 설치되는 전자정보처리조직을 사용하여, 이하에 게기하는 요건에 해당하는 번호를 생성하고 신속하게 당해 시정촌(市町村)

7) 고도전문직 제2호란 일본의 학술연구나 경제발전에 기여할 것이 예상되는 고도의 전문적인 능력을 가진 외국인의 유입을 보다 촉진하기 위해 재류기간 5년의 '고도전문직 1호' 또는 고도인재 외국인으로서의 '특정 활동'의 재류자격으로 일정기간 재류한 자를 대상으로 재류기한을 무기한으로 하고 활동제한을 크게 완화한 재류자격으로서 마련한 것을 가리킨다.

8) 지방자치법 2조 8항의 규정에서, 지방공공단체의 사무에는 ①지역에서의 사무, 이른바 자치사무와 ②법정수탁사무의 2종류가 된다. 법정수탁사무에 대해서는 동법 2조 9항 및 10항이 이를 규정하고 있다. 지방자치법 14조에 따라 지방공공단체는 법령에 위반되지 않는 한 지방자치법 2조 2항의 사무에 관해 조례를 제정할 수 있다고 규정되어 있다. 이 점에 있어서는 법정수탁사무란 법해석상 자치사무와 다른 것으로서 취급될 필요가 없다고 할 수 있다. 그런데 실정법의 많은 규정(지방자치법 245조의7에 규정하는 '시정 지시' 및 동조의8에 규정하는 '대집행 등')에서 보듯이 법정수탁사무의 처리시에는 자치사무의 처리와는 분명히 다른 국가 등의 관여수법이 규정되어 있다.

9) 人見剛「番号法における個人番号制度をめぐる問題」法律時報 88巻 4号(2016年) 1頁

의 장에 대해 통지하도록 한다(동조 2항). 그 요건이란 ① 다른 어떠한 개인번호(전조 제2항의 종전의 개인번호를 포함)와도 다를 것 ② 전항의 주민표 코드를 변환시켜 얻을 수 있는 것일 것 ③ 전호의 주민표 코드를 복원할 수 있는 규칙성을 갖춘 것이 아닐 것 등으로 되어 있다. 그리고 이상의 기구는 전항의 규정에 따라 개인번호로 할 번호를 생성하고 아울러 당해번호의 생성 및 시정촌(市町村)의 장에 대한 통지에 대해 관리하기 위한 전자정보처리조직을 설치하는 것으로 되어 있다(동조 3항).

개인번호법 7조에 따라 시정촌(市町村)의 장(특별구의 구장(区長)을 포함. 이하, 동일)이 주민기본대장법 제30조의3 제2항의 규정에 따라 주민표에 주민표 코드를 기재한 때는, 정령에서 정하는 바에 따라 신속하게 다음 조(条) 제2항의 규정에 따라 기구로부터 통지받은 개인번호로 할 번호를 그 자의 개인번호로 지정하고 그 자에 대해 당해 개인번호를 통지카드(성명, 주소, 생년월일, 성별, 개인번호 기타 총무성령에서 정하는 사항이 기재된 카드를 말한다. 이하 동일)에 의해 통지하여야 한다(법 7조 1항). 시정촌(市町村)의 장은, 당해 시정촌(市町村)(특별구를 포함. 이하, 동일)이 비치하는 주민기본대장에 기록되어 있는 자의 개인번호가 유출되어 부정하게 사용될 염려가 있다고 인정되는 때는 정령에서 정하는 바에 따라 그 자의 청구 또는 직권으로 그 자의 종전의 개인번호 대신에 다음 조(条) 제2항의 규정에 따라 기구로부터 통지받은 개인번호로 할 번호를 그 자의 개인번호로 지정하고 신속하게 그 자에 대해 당해 개인번호를 통지카드에 의해 통지하여야 한다(동조 2항).

3. 개인번호 카드

2016년 1월부터 본인의 신청에 의한 개인번호 카드의 교부가 개시되고 있다. 개인번호 카드는 개인번호를 증명하는 서류와 본인확인 당시의 공적인 신분증명서로서 이용될 수 있고 또한 다양한 행정서비스를 받을 수 있게 되는 IC카드를 가리킨다. 교부 수수료는 당분간 무료이다(본인의 귀책사유로 인한 재발행의 경우를 제외). 앞면에는 성명, 주소, 생년월일, 성별, 얼굴사진, 전자증명서의 유효기간의 기재란, 보안코드, 서명패널영역(이사한 경우의 새주소 등), 장기제공의사 표시란이 기재되고 개인번호는 뒷면에 기재되어 있다.

개인번호 카드는 금융기관 등 본인확인이 필요한 창구에서 신분증명서로서 이용될 수 있지만, 개인번호를 복사·보관할 수 있는 사업자는 행정기관과 고용주 등 법령에 지정된 자로 한정되어 있기 때문에 지정되어 있지 않은 사업자의 창구에서 개인번호가 기재되어 있는 카드의 뒷면을 복사·보관할 수는 없다.

개인번호 카드의 교부 등에 관한 법제에 대해 살펴보면, 시정촌(市町村)의 장은 정령에서 정

하는 바에 따라 당해 시정촌(市町村)이 비치하는 주민기본대장에 기록되어 있는 자에 대해, 그 자의 신청에 따라 그 자에 관련된 개인번호 카드를 교부하기로 한다. 이 경우에 당해 시정촌(市町村)의 장은 그 자로부터 통지카드의 반납 및 전조의 주무성령에서 정하는 서류의 제시를 받거나 또는 동조의 정령에서 정하는 조치를 취하여야 한다(법 17조 1항). 개인번호 카드의 교부를 받은 자가 주민기본대장법 제24조의2 제1항에 규정하는 최초의 전입신고를 하는 경우에는 당해 최초의 전입신고와 동시에 당해 개인번호 카드를 시정촌(市町村)의 장에게 제출하여야 한다(동조 2항). 전항의 규정에 따라 개인번호 카드의 제출을 받은 시정촌(市町村)의 장은 당해 개인번호 카드에 대해 카드기록사항의 변경 기타 당해 개인번호 카드의 적절한 이용을 확보하기 위해 필요한 조치를 마련하고 이를 반환하여야 한다(동조 3항). 제2항의 경우를 제외하고, 개인번호 카드의 교부를 받은 자는 카드기록사항에 변경이 있는 때는 그 변경이 있은 날부터 14일 이내에 그 뜻을 주소지인 시정촌(市町村)의 장에게 신고함과 아울러 당해 개인번호 카드를 제출하여야 한다. 이 경우에는 전항의 규정을 준용한다(동조 4항). 개인번호 카드의 교부를 받은 자가 당해 개인번호 카드를 분실한 때는 즉시 그 뜻을 주소지인 시정촌(市町村)의 장에게 신고하여야 한다(동조 5항). 개인번호 카드는 그 유효기간이 만료된 경우 기타 정령에서 정하는 경우에는 그 효력을 상실한다(동조 6항). 개인번호 카드의 교부를 받은 자는 당해 개인번호 카드의 유효기간이 만료된 경우 기타 정령에서 정하는 경우에는 정령에서 정하는 바에 따라 당해 개인번호 카드를 주소지인 시정촌(市町村)의 장에게 반납하여야 한다(동조 7항). 앞의 각 항에 규정한 것 이외에 개인번호 카드의 양식, 개인번호 카드의 유효기간 및 개인번호 카드의 재교부를 받으려는 경우의 절차 기타 개인번호 카드에 관해 필요한 사항은 총무성령으로 규정한다(동조 8항).

4. 공적 개인인증서비스의 전자증명서

공적 개인인증서비스의 전자증명서는 시구정촌(市区町村) 창구에서 발행된 때에 개인번호카드(IC카드) 안에 기록하여 인도하게 된다. 전자증명서는 개인번호 카드 안에 내장되기 때문에 이미 개인번호 카드를 취득한 사람은 지참하고, 아직 개인번호 카드를 취득하지 않은 사람은 개인번호 카드를 먼저 취득해야 한다. 많은 시구정촌(市区町村)에서는 동일 창구에서 개인번호 카드와 전자증명서의 발행이 이루어지고 있다. 동 증명서는 법률에 근거하여 '지방공공단체 정보시스템기구'가 운영하는 시스템으로 신뢰성이 높은 전자증명서를 이용자들에게 제공함으로써 국가와 지방공공단체가 제공하고 있는 온라인 신청을 안전하게 수행하기 위한 것이다. 결국, 국민은 공적 개인인증서비스로 발행된 전자증명서를 이용하여 행정기관 등이 제공하고 있는 인

터넷을 이용한 전자신청과 신고 서비스 등을 이용할 수 있다. 이를 이용하기 위해서는 전자증명서의 발행은 물론 IC카드Reader·Writer가 필요하다. 이 IC카드Reader·Writer란 IC카드에 기록된 전자정보를 읽기위한 기기이다. 이처럼 공적 개인인증서비스를 이용한 온라인에 의한 행정절차를 밟기 위해서는 전자신청 등에 이용할 인터넷에 접속된 컴퓨터와, 컴퓨터로 전자증명서를 이용하기 위해 필요한 IC카드Reader·Writer의 준비가 필요하다.

개인번호 카드 이용 시의 보안대책에 관해서는 액세스권의 제어가 이루어지고 있고, IC칩 내부의 각 어플리케이션 사이는 '어플리케이션 Firewall'에 의해 독립되어 있으며, 어플리케이션마다 조건과 비밀번호 등의 액세스권 정보를 설정함으로써 각 서비스용 시스템에서 다른 어플리케이션으로 액세스하는 것을 제어하고 있다. 어플리케이션 마다 다른 비밀번호를 설정하여 정보를 보호하고 또한 비밀번호의 입력을 일정 횟수이상 잘못하면 카드가 잠기는 구조로 되어 있다. 그리고 보안대책으로서 내(耐)탬퍼성(性)(tamper resistence)[10]이 제시되고 있다. 개인번호 카드의 IC칩은 이러한 위조목적의 부정행위에 대한 내(耐)탬퍼성(性)을 가지고 있어서 높은 보안성을 확보하고 있다고 설명된다.

5. 개인번호 카드와 주기카드와의 차이점에 대하여

1999년의 주민기본대장법(이하 '주기법'이라 한다) 개정과 그 후 2003년 8월 25일에 개시된 주민기본대장카드의 교부, 그 이듬해부터 동 카드에 입력된 전자증명서와 현재의 개인번호 카드와의 사이에는 다음과 같은 차이점이 있다[11].

10) 내(耐)탬퍼성이란 IC칩 내부의 정보가 부정하게 읽혀진다거나 해석되려고 한 경우, 자동적으로 내용이 소거되는 등의 대항조치가 마련되는 성질이다.

11) 이것은 총무성의 홈페이지; 총무성 top > 정책 > 지방행재정 > 개인번호제도와 개인번호카드 > 개인번호카드 (http://www.soumu.go.jp/kojinbango_card/03.html).

[주민기본대장 카드와 My Number 카드의 비교]

	주민기본대장 카드	My Number 카드
1. 권면의 기재내용	• 주민표 코드의 권면기재 없음 • 얼굴사진은 선택제	• 개인번호를 권면에 기재(뒷면) • 얼굴사진을 권면에 기재
2. 전자증명서	• 서명용 전자증명서 (e-Tax에서의 확정신고 등의 전자신청에 사용)	• 서명용 전자증명서 • 이용자증명용 전자증명서(신규)(편의점 교부 및 마이나포탈의 로그인 등 본인 인증수단으로서 사용)
3. 수수료 (전자증명서)	주로 500엔 (전자증명서를 게재한 경우는 1000엔)	무료(전자증명서 포함)
4. 유효기간	• 발행일부터 10년 *전자증명서(서명용)는 3년	• 발행일부터 신청자의 10회째 생일까지 (다만, 20세 미만인 자는 용모의 변화가 크므로 신청자의 5회째 생일까지) *전자증명서(서명용·이용자증명용)는 발행일부터 5회째의 생일까지
5. 편리성	• 신분증명서로서의 이용이 중심 • 시정촌(市町村)에 의한 부가서비스의 이용(편의점 교부, 도서관 이용 등)	• 신분증명서로서의 이용 • 개인번호를 확인하는 경우의 이용(취직, 전직, 출산육아, 질병, 연금수급, 재해 등) • 시정촌(市町村), 도도부현(都道府県), 행정기관 등에 의한 부가서비스의 이용 (도서관 이용 기타 건강보험증, 국가공무원신분증 등) • 편의점 교부 이용의 확대(이용자증명용 전자증명서의 활용에 의함) • 전자증명서에 의한 민간부문을 포함한 전자신청·거래 등에서 이용

Ⅳ. 개인정보보호와 개인번호의 이용

1. 개인정보보호 법제도에 대하여

개인정보의 보호에 관한 법률[12]은 개인 식별부호가 포함된 것까지도 개인정보로서 보호의 대상으로 하였다. 종래, 개인정보보호법 2조 1항에 따라 '개인정보'란 생존하는 개인에 관한

12) 개인정보보호법은 2015년 9월 9일에 그 개정법(2015년 9월 9일 법률 제65호)이 공포되고 2016년 1월 1일에 그 일부가 시행되며, 또한 공포일부터 기산하여 2년을 넘지 않는 범위 내에서 정령으로 정하는 날에 전면시행 하기로 되어 있다. 동 개인정보보호법은 2015년 9월 9일에 개인정보의 보호에 관한 법률 및 개인번호법의 일부를 개정하는 법률안이 성립하여 공포된 것에 따른 것이다.

정보로서 당해 정보에 포함되는 성명, 생년월일 기타 기술 등에 의해 특정 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조하여 확인할 수 있고 그럼으로써 특정 개인을 식별할 수 있게 되는 것을 포함)으로 정의되어 있었다. 그런데 개정 개인정보법 2조 1항은 '개인정보'에 대해서, 생존하는 개인에 관한 정보로서 ① 당해 정보에 포함되는 성명, 생년월일 기타 기술 등(문서, 도화 혹은 전자적 기록(전자적 방식(전자적 방식, 자기적 방식 기타 사람의 지각으로는 인식할 수 없는 방식을 말한다. 다음 항 제2호에서도 동일)으로 만들어지는 기록을 말한다. 제18조 제2항에서도 동일)에 기재되거나 혹은 기록되거나 또는 음성, 동작 기타 방법을 이용하여 나타낸 일체의 사항(개인 식별부호를 제외)을 말한다. 이하 동일)에 의해 특정 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조하여 확인할 수 있고 그럼으로써 특정 개인을 식별할 수 있게 되는 것을 포함) ② 개인 식별부호가 포함되는 것으로 정의하고 이들을 보호의 대상으로 하고 있다.

그리고 '개인 식별부호'에 대해서는 동법 2조 2항이 다음 각 호의 어딘가에 해당하는 문자, 번호, 기호 기타 부호 중 정령에서 규정하는 것이라고 정의하고 있다. 그 각 호에는 ① 특정 개인의 신체 일부의 특징을 전자계산기용으로 제공하기 위해 변환시킨 문자, 번호, 기호 기타 부호로서, 당해 특정 개인을 식별할 수 있는 것 ② 개인에게 제공되는 서비스의 이용 혹은 개인에게 판매되는 상품의 구입에 관해 배정되거나 또는 개인에게 발행되는 카드 기타 서류에 기재되거나 혹은 전자적 방식에 의해 기록된 문자, 번호, 기호 기타 부호로서, 그 이용자 혹은 구입자 또는 발행을 받는 자마다 다른 것이 되도록 배정되거나 또는 기재되거나 혹은 기록됨으로써 특정 이용자 혹은 구입자 또는 발행을 받는 자를 식별할 수 있는 것이 열거되어 있다.

이상의 개인정보보호법2조 2항 1호에 해당되는 것으로는 지문인식데이터, 얼굴인식데이터가 포함되고, 동항 2호에서 말하는 개인 식별부호, 즉 개인에게 발행되는 카드 기타 서류에 기재되는 번호로서 여권번호, 면허증번호 등이 포함되어 있으며, 개인 식별부호가 될지 어떨지 여부에 관한 판단요소로서는 일의성(개인과의 부합상태가 일대일인지 어떤지), 불변성(부호의 변경이 빈번히 이루어지지 않는지), 본인도달성(부호를 토대로 직접 개인에게 접근할 수 있는지)이 있다는 내용이 제시되었다[13].

위에서 본 것처럼, 개인정보보호법 2조 2항은 그 1호 및 2호에서 개인 식별부호에 대해서, 정보개체로 특정 개인을 식별할 수 있는 것이라고 정의하면서 게다가 정령에서 이들을 규정한다고 하고 있다. 동 정령에서 규정하여 개인정보 해당성을 객관화함으로써 문자, 번호, 기호 기타 부호 등 정보가 보호의 대상이 되는지 아닌지에 관한 사업자의 판단이 용이하게 되도록

13) 座談会「個人情報保護法・個人番号法改正の意義と課題」ジュリスト 2016年 2月号 16頁

한 것이다[14].

그리고 동법 2조 3항은 '배려요망 개인정보'를 규정하고 있다. 배려요망 개인정보란 본인의 인종, 신조, 사회적 신분, 병력, 범죄경력, 범죄에 의해 피해를 입은 사실 기타 본인에 대한 부당한 차별, 편견 기타 불이익이 발생하지 않도록 그 취급에 특히 배려가 필요한 것으로서 정령에서 규정하는 기술 등이 포함되는 개인정보라고 정의되어 있다. 동 배려요망 개인정보에 대해서는, 개인정보 사업자는 ① 법령에 근거한 경우 ② 사람의 생명, 신체 또는 재산의 보호를 위해 필요가 있는 경우로서 본인의 동의를 얻는 것이 곤란한 때 ③ 공중위생의 향상 또는 아동의 건전한 육성을 추진하기 위해 특히 필요한 경우로서 본인의 동의를 얻는 것이 곤란한 때를 제외하는 경우 외에, 미리 본인의 동의를 얻지 않고 배려요망 개인정보를 취득해서는 아니 된다(동법 17조 2항).

또한 개인정보보호법 2조 9항은 '익명가공정보'에 대해서, 다음 각 호에 게기하는 개인정보의 구분에 따라 당해 각 호에 규정하는 조치를 마련하고 특정개인을 식별할 수 없도록 개인정보를 가공하여 얻을 수 있는 개인에 관한 정보로서, 당해 개인정보를 복원할 수 없도록 한 것이라고 정의하고 다음의 각 호로서는 ① 제1항 1호에 해당하는 개인정보 : 당해 개인정보에 포함되는 기술 등의 일부를 삭제할 것(당해 일부의 기술 등을 복원할 수 있는 규칙성이 없는 방법으로 다른 기술 등으로 치환하는 것을 포함) ② 제1항 제2호에 해당하는 개인정보 : 당해 개인정보에 포함되는 개인 식별부호의 전부를 삭제할 것(당해 개인 식별부호를 복원할 수 있는 규칙성이 없는 방법으로 다른 기술 등으로 치환하는 것을 포함)을 열거하고 있다.

위에서 본 것처럼, 개인정보보호법은 개인정보의 목적 외 이용과 개인데이터(개인정보데이터베이스 등을 구성하는 개인정보, 이에 대해서는 동법 2조 6항)의 제3자 제공을 위해서는 원칙적으로 사전에 본인의 동의를 얻어야 한다. 그러나 수백만 명의 개인정보를 취급하는 자, 이른바 개인정보취급사업자에게 모든 사람의 동의를 얻을 것을 요구하는 것은 시간적·경제적으로 무리한 경우도 있음을 부정할 수 없다. 그러므로 개인정보보호법은 개인의 권익을 침해하는 일이 없도록 하면서 방대한 데이터를 활용할 수 있도록 익명가공정보[15]에 관한 제도를 마련한 것이다. 즉, 개인정보보호법은 이용목적의 특정과 제3자 제공의 제한 등 개인정보의 취급 시에 요구되는 의무의 적용제외가 될 수 있게, 개인이 특정될 수 없도록 데이터를 가공·처리한 '익명가공정보'라고 하는, 개인정보와는 다른 새로운 퍼스널데이터의 구분을 마련하기로 한 것이

14) 日置巴美「改正個人情報保護法の概要」前掲 ジュリスト 31頁

15) 익명가공정보의 활용사례로서는 GPS에 의해 취득된 위치정보나 교통관련 IC카드의 승강이력 등, 물품구입이력, 의료기관이 보유하는 의료정보 등이 있고, 이들 정보에 대해서 개인이 특정될 수 없도록 데이터를 가공 처리한 '익명가공정보'로 하여, 동 정보를 도시개발이나 상품개발에 복수의 업자 사이의 분야횡단적인 이용을 하는 경우가 있을 것이다.

다. 익명가공정보의 작성방법은 신설되는 개인정보보호위원회가 그 기준을 정하기로 되어 있다(동법 36조 참조).

물론 개인정보보호법은 개인정보의 제3자에의 제공을 원칙적으로 제한하고 있다. 즉, 개인정보취급사업자는 ① 법령에 근거한 경우 ② 사람의 생명, 신체 또는 재산의 보호를 위해 필요가 있는 경우로서 본인의 동의를 얻는 것이 곤란한 때 ③ 공중위생의 향상 또는 아동의 건전한 육성을 추진하기 위해 특히 필요한 경우로서, 본인의 동의를 얻는 것이 곤란한 때 ④ 국가기관 혹은 지방공공단체 또는 그 위탁을 받은 자가 법령에 정한 사무를 수행하는 것에 대해 협력할 필요가 있는 경우로서, 본인의 동의를 얻음으로써 당해 사무의 수행에 지장을 초래할 염려가 있는 때를 제외한 경우 외에 미리 본인의 동의를 얻지 아니한 채 개인데이터를 제3자에게 제공해서는 아니 된다(동법 23조 1항).

이에 더하여 개인정보보호법 제4장 제1절에는 개인정보취급사업자의 의무가 제2절에는 익명가공정보취급사업자 등의 의무가 규정되어 있다. 동 위원회의 개인정보취급사업자 또는 익명가공정보취급사업자에 대한 감독권한 등에 대해서는, 개인정보보호법 제4장 제3절의 40조 내지 42조가 이를 규정하고 있다. 같은 장(章) 4절에는 민간단체에 의한 개인정보의 보호추진이 규정되어 있다. 개인정보보호위원회의 구성 내지 조직 등에 관해서는 개인정보보호법 제5장이 이를 규정하고 있다. 동 위원회는 개안정보의 취급을 감시·감독할 권한을 가진 제3자 기관이다.

2. 개인번호 이용을 위한 법제

한편, 개인번호의 이용에 관해서는 개인번호법 9조가 개인번호 이용을 위한 근거규정이다. 개인번호이용사무 또는 개인번호관계사무(이하, '개인번호이용사무 등'이라 한다)의 전부 또는 일부의 위탁을 받은 자는 당해 개인번호이용사무 등의 위탁을 한 자의 허락을 얻은 경우에 한하여 그 전부 또는 일부의 재(再)위탁을 할 수 있다(동법 10조 1항).

그리고 동법 19조가 특정 개인정보의 제공을 위한 근거규정을 두고 있다. 동 규정은 다른 분야에 속하는 정보를 대조하고 확인하는 데이터 조합(Matching)을 가능하게 하는 것이다. 그런데 동법 19조가 "누구든지 다음 각 호의 어딘가에 해당하는 경우를 제외하고 특정개인정보의 제공을 해서는 아니 된다"고 규정하고, 그 근거규정이 제1호 내지 제13호까지의 개별영역을 제시하면서 제14호("사람의 생명, 신체 또는 재산의 보호를 위해 필요한 경우에, 본인의 동의가 있거나 또는 본인의 동의를 얻는 것이 곤란한 때") 및 제15호("기타 이들에 준하는 것으로서 개인정보보호위원회규칙에서 정하는 때")라고 하는 예시 열거의 형태를 취하고 있으며, 그 이용의 영역확대가 법률이 아닌 개인정보보호위원회규칙에 의해 가능한 것으로 되어 있다.

이 점에서 보면, 특정개인정보 개인번호의 무절제한 제공확대가 염려될 수 있다. 그리고 2015년 9월 9일에 개인정보의 보호에 관한 법률 및 개인번호법의 일부를 개정하는 법률안이 성립되고 공포되어 동법에 따라 개인정보보호법 및 개인번호법의 일부 개정 외에 지방세법, 후생연금보험법, 극민연금법, 국세통칙법, 등록면허세법, 주민기본대장법, 에너지 사용의 합리화 등에 관한 법률, 조직적인 범죄의 처벌 및 범죄수익의 규제 등에 관한 법률, 민간사업자 등이 행하는 서면보존 등에서 정보통신기술의 이용에 관한 법률, 유실물법 등을 개정하고 개인번호의 이용을 목적으로 하는 법이 개정된 것이다. 이러한 법들의 개정으로 예컨대, 원천징수, 지불조서, 고용보험 피보험자자격취득신고, 건강보험 피보험자자격취득신고, 후생연금보험 피보험자자격취득신고 등에 개인번호의 이용이 의무화되어 있다. 사회보험과 원천징수표, 법정조서 등의 각종 행정기관에의 제출서류에는 개인번호, 법인번호의 기재가 요구되므로 모든 종업원과 그 가족의 개인번호정보를 기업 스스로 수집하고 다양한 엄격한 규칙에 따라 적절히 관리할 필요가 있다. 이 때문에 개인번호법은 특정개인정보의 취급에 관한 감독 등에 관한 제6장을 새로 마련하였다.

Ⅴ. 맺으며-개인번호제에 따른 국민의 편리성과 행정의 효율화

총무성의 홈페이지[16]에 의하면, 이미 주기네트의 시행에 관한 평가로서 주민의 편리성 향상과 행정의 효율화가 도모되었다고 하는 장점이 제시되고 있다.

또한 개인번호 카드의 취득자가 동 카드를 이용하는 것의 장점에 대해서 총무성의 홈페이지에 따르면[17], 다음과 같이 설명되어 있다. 즉, 개인번호제도 도입 후는 취직, 전직, 출산육아, 질병, 연금수급, 재해 등 많은 상황에서 개인번호의 제시가 필요해진다. 그 때, 통지카드라면

16) 총무성 Top> 정책> 지방행재정> 주민기본대장 등> 주기네트> 주기네트로 가능해진 것은?> 주지네트의 장점에 대하여 (http://www.soumu.go.jp/main_sosiki/jichi_gyousei/daityo/01_merit.html). 총무성에 따르면, ① 주기네트는 고령자를 중심으로 매우 도움이 되고 있다. 연금수급자는 생존확인을 위해 매년 '현황신고'라 불리는 신고를 하여야만 하는데, 주기네트의 활용으로 2006년 10월부터 생략할 수 있도록 되어 있다. 전국에서 4천만 명이 이 편리함을 누리고 있다. 신고서에 기입하여 50엔 우표를 붙여 우체통에 넣는 것은 그다지 힘들지 않다는 지적도 있다. 그러나 힘든 정도는 사람마다 다르다. 나이가 들수록 더 그렇다. 주기네트는 이러한 국민부담을 줄이기 위해 있어야 하는 것이다. 주기네트의 편리성을 제시한다. ② 신분증명서로서의 주기카드의 유효성에 대해서는, 주기카드는 전국에서 약 764만 매(2013년 6월 현재). 아직도 보급이 충분치 않다. 그러나 다양한 사정으로 운전면허가 없는 사람, 고령자가 되어 운전면허증을 반납한 사람 등으로서는 주기 카드는 신분증명서로서 매우 귀중한 존재이다. ③ 전자신청을 이용함으로써 의료비공제절차가 용이해지는 편리성을 제시하고 있다. 의료비공제를 매년 확정 신고하는 사람도 많다. 그 때, 신고서에 영수서를 붙이는 것이 수고스럽다. 주기카드에 내장된 공적 개인인증서비스의 전자증명서를 이용하여 e-Tax에 의한 확정 신고의 전자신청을 하는 경우에는, 영수서는 보존하면 되는 것으로 되어 있어서 첨부가 필요 없다. 또한 세액공제를 받을 수가 있다.

17) 앞의 주 4 참조

운전면허증과 여권 등 다른 본인확인서류가 필요하게 되지만, 개인번호 카드가 있으면 한 장으로 번호확인과 본인확인이 가능해진다. 그밖에도 개인번호 카드를 취득하면 ①본인확인시의 공적인 신분증명서로서 이용할 수 있고 ②시구정촌(市区町村)과 국가 등이 제공하는 다양한 서비스마다 필요했던 복수의 카드가 개인번호 카드와 일체를 이루게 되는데, 예컨대 지방공공단체의 인감등록증과 도서카드로서의 이용가능, 민간에서의 포인트 카드, 입퇴자(入退者)관리와 신분증으로서 이용가능 ③2017년 1월부터 개시되는 마이나 포탈에의 로그인을 비롯하여 각종 행정절차의 온라인신청에 이용될 수 있게 되는 점 ④온라인 뱅킹을 비롯하여 각종 민간의 온라인거래에 이용할 수 있게 되는 점 ⑤편의점 등에서 주민표, 인감등록증명서 등의 공적인 증명서를 취득할 수 있게 되는 등 매우 다양한 장점을 누릴 수 있게 될 전망이 있다는 설명이 있다.

확실히 주민표의 취득 및 은행계좌 개설 등의 경우에, 관공서나 은행까지 가지 않은 채 컴퓨터나 스마트 폰 등을 이용하여 이러한 절차들을 밟을 수가 있다고 하는 편리함을 국민이 누릴 수 있다. 이러한 편리성을 살리기 위해서는 특히 고령화 사회의 고령자가 인터넷 사용법에 익숙해져 있을 것이 대전제가 될 것이다.

그런데 실제로 많은 국민은 일회의 주민표나 인감등록증의 발행을 위해, 개인번호 카드의 교부를 위한 신청을 하지는 않을 것으로 생각된다. 그렇다면 이러한 개인번호 카드의 취득에 따른 국민의 편리성 증진이란 그림 속의 떡이고 많은 국민이 이 편리함을 누리게 되지는 않는다[18]. 바꾸어 말하면, 국가가 개인번호를 통해 세금의 정확한 징수나 생활보호 등의 급부행정상 결정의 정확도를 도모할 수 있다고 하는 점에 개인번호제의 장점이 있는 반면, 개인번호의 활용 등에 관해서는 거짓행세와 같은 부정이용의 가능성, 정보유출의 위험성, 정부에 의한 주민감시 등의 단점도 있을 것이다. 이러한 단점을 생각하면, 개인번호제가 '국가로부터의 자유'라는 '고전적인' 자유에 대한 '침식'이 된다는 식의 과장된 표현은 정보화 사회라는 시대의 흐름에 역행하는 일이 될 것인가.

또한 개인번호제는 당초 세금과 사회보장의 일체적 개혁을 목적으로 하여 그들 분야에 제한적으로 이용하기 위해 고안되었는데, 그 후 동일본 대지진의 경험을 반영하여 재해분야가 추가되었다. 이후 재판절차, 형사사건 수사에서의 이용까지 포함하여 법정되어 있다(개인번호법 19조 12호·9조 5항). 더구나 개인번호·법인번호의 이용에 관해서는 사회보장·세금·재해대책 이외의 분야, 즉 다른 행정분야 및 행정분야 이외의 국민편익의 향상에 기여하는 분야에서의 이용

18) 개인이 행정절차를 밟는 상황은 일평생동안 그다지 많지 않고, 행정절차를 밟는 경우의 첨부서류 삭감이라는 장점을 위해 큰 금액의 세금을 투입하여 번호 제도를 도입하는 것은 무의미하다는 지적도 있다(水町雅子「やさしい番号法入門」(商事法務, 2014) 67頁).

가능성을 고려하여야만 한다는 개인번호법 3조 2항, 개인번호 카드의 이용에 관해서는 행정사무 이외의 사무처리에서 개인번호 카드의 활용이 도모되도록 해야 한다는 동법 3조 3항, 또한 정보제공 네트워크시스템에 관해서는 특정개인정보 이외의 정보의 수수에 정보제공 네트워크시스템의 용도를 확대할 가능성을 고려해야만 한다는 동법 3조 4항은 개인번호의 이용촉진법으로서 개인번호법의 기본이념을 규정하고 있는 것이기는 해도, 이러한 것들이 개인정보보호법제(특히 개인정보보호법 15조·16조, 행정기관 개인정보보호법 3조·4조·8조)에 커다란 바람구멍이 뚫리고 이것이 무절제하게 확대되는 일이 크게 염려된다는 점이 지적되었다[19]. 마찬가지로 개인번호법은 특정개인정보의 활용을 중시하고 있으므로 특별법인 개인번호법이 기본법인 개인정보보호법상의 보호목적을 완화하고 활용을 우선시키는 것이 타당한지 하는 질문에 대해, 개인번호법의 입법자 의사로서 "법안의 구체적인 조문은 결코 보호를 느슨하게 하는 것이 아니고 오히려 이용에 대한 제약을 엄격하게 한 측면이 있으며, 또한 특히 조직측면에서는 제3자 위원회로서의 개인정보보호위원회를 두고 그 독립성을 확보하고 있으므로, 개인의 권리이익의 침해는 허용되지 않는다는 전제는 기본법특별법에 공통된다고 해석해야 한다"는 입법자의 견해가 표명되어 있다[20]. 특히, 지방공공단체는 ① 이미 My Number 이용 사무로 되어 있는 공영주택(저 소득자 대상)의 관리에 더하여 특정우량임대주택(중 소득자 대상)의 관리에서 개인번호의 이용이 가능하다고 하였고 ② 지방공공단체가 조례로서 독자적으로 My Number를 이용하는 경우에도 정보제공 네트워크시스템을 이용한 정보연계를 가능하다고 보고 ③ 지방공공단체의 요망 등을 반영하여 고용, 장애자복지 등의 분야에서 이용사무, 정보연계를 추가하기로 되어 있다[21]. 이러한 지방공공단체의 개인번호 이용은 지방공공단체가 종합행정의 주축이라는 점에서 비롯된 이용모습이지만, 이에 대해서는 지방공공단체에 의한 개인정보의 집적과 확대가 염려된다. 이러한 우려에 대해서는 "과세의 적정화에 대해서 말하자면, 개별 매매에 대해서 개인번호가 붙은 영수서(領収書)를 작성하고 이를 신고하는 것을 의무로 하고 있는 것이 아니므로 사업소득의 파악에는 한계가 있다. 사회보장에 대해서도 소득뿐만 아니라 자산까지 파악하지 않으면 진정으로 손길이 필요한 자를 확정할 수 없는데, 현행 번호제도에서는 자산의 파악까지 가능한 것은 아니다"라는 일정한 한계가 있음을 제시한 견해가 있다[22].

---

19) 人見剛「番号法における個人番号制度をめぐる問題」法律時報 88巻 4号(2016年) 2頁

20) 亘理格 등「質疑応答の概要」法律時報 88巻 1号(2016年) 86頁. 이 질의응답이란 제15회 행정법연구포럼에서 이루어진 것이다.

21) 内閣府大臣官房番号制度担当室「個人情報の保護に関する法律および個人番号法の一部を改正する法律案(概要)」2015년 2월 16일. 동 자료에 따르면, 『世界最先端IT国家創造宣言』 (2014年6月24日 閣議決定) 등을 반영하여 보다 효율화·편리성의 향상이 예상되는 분야에 대하여 My Number의 이용범위 확대나 제도기반의 활용을 도모함과 동시에 My Number제도의 주축인 지방공공단체의 요망 등을 반영하여 소정의 정비를 하기로 되어 있다.

어쨌든, 정보화 사회의 진전에 따른 개인번호제는, 현 시점에서 행정사무의 효율화를 도모하는 것으로서 그 필요성을 부정할 수 없다. 하지만 앞으로 반드시 개인번호제의 이용확대가 한층 진행될 것이라는 전제에서 본다면, 일본의 개인번호제 시행이 '민주사회'에서 '감시사회'로 가는 출발점이 되지 않도록 개인번호제의 엄격한 운용을 통제할 법제도가 무엇보다 중요할 것이다.

이상 경청해주셔서 감사합니다.

(2016.5.31. 탈고)

22) 宇賀克也「番号制度導入の意義と実務上の留意点」自治実務セミナー 644号(2016年2月) 3頁

Session 2

미국과 대만의 개인식별번호법제의 현황과 문제점

Session 2-1

미국의 개인식별번호법제 현황과 문제점

Erin Murphy | 영남대학교 교수

Legal issues regarding Individual Identifiable Numbering Systems in the United States

Ⅰ. Introduction

The United States does not have an individual identification numbering system. The Social Security number, which has been utilized as the de facto identification system, was originally designed to be a numerical system for tracking Social Security. Ones' social security number has essentially attained the purpose of a universal identification number. This was not the purpose of the Social Security Program and it is also not an effective national identification system.

The United States government has long debated implementing a national identity management system. Politicians and proponents of such identification programs claim that this system would benefit combatting terrorism, protect the people from identity theft, aid in travel, and also help monitor legal employment, identify illegal employment and benefit fraud.

Opponents of national identification management systems argue that this type of system would not solve many of the problems that the government has specified would be solved should this plan be implemented; more specifically, that it would not reduce terrorism. In addition, general privacy concerns, enhanced surveillance and monitoring of citizens and increased risk of identity theft, are concerns many have should there be a national identification number database implemented.

This article will explore the history of the United States identification systems, starting with the Social Security numbering system; how it went from a way to track employment and retirement savings to a quasi-universal identification number. The article will also review the REAL ID Act, which was passed in 2005, and the implementation by states of these new regulations on driver's licenses. While explaining the history, I will also analyze the legal issues with the current use of the Social Security numbers and the REAL ID Act, legislation that has been passed to protect citizens from misuse and the constitutionality of national identification numbering systems. It is clear that The United States is divided on this issue and that true implementation of a national identification program is not an imminent reality.

Ⅱ. History of Social Security Numbers

Social Security is a social insurance program, started by the Social Security Administration program as part of the New Deal, the Social Security Act, which was passed in 1935.[1] The Social Security Number, created a year after the program was started, was implemented for the purpose of tracking Social Security benefit entitlement. Social Security meant to be a social insurance program, to pay retired workers age 65 or older a continuing income, based on their previous earnings.[2] Gradually, Social Security has also included providing benefits to disabled people, and families of retired, disabled or deceased workers.

In June, 1936, The Social Security Board decided on a nine digit scheme, the first three numbers representing a geographic region number, the next two numbers were a group number, which was initially determined by the procedure of issuing numbers in groups of 10,000 to post offices, sequenced beginning with odd-numbered groups (01-09) and then following even numbered groups (10-98), then finally odd numbers (11-99). The last four digits are the serial number, a straight numerical series of numbers from 0001-999 within each group.[3]

Starting in November 1936, post offices started the registration of social security numbers by disseminating of application forms to employers based on lists provided by postmen who made up lists of employers on his or her routes. This was about 2.4 million employers at the time.[4] As of December 2008, the Social Security Administration had issued over 450 million original social security numbers, with almost all legal residents in the United States having one.

At first, only employees working in covered employment and 64 years or younger were eligible to obtain a social security number, but after problems with preferential hiring for those who were already enrolled in social security started to occur, the Social Security Bureau began to issue a Social Security Number to anyone who applied. [5]

The social security number card, alone, does not serve proof of identity. [6] In fact, for many years,

---

1) Puckett, Carolyn, The story of the Social Security Number, Social Security Bulletin, Vol. 69, No. 2, 2009. https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

2) Historical Background and Development of Social Security, https://www.ssa.gov/history/briefhistory3.html

3) Id.

4) McKinley, Charles, and Robert W. Frase. Launching Social Security: A capture-and-record account, 1935–1937. Madison, WI: The University of Wisconsin Press, 344-45 and 368, 1970.

5) History of SSA 1993 - 2000, Chapter 6: Program Integrity. Available at: http://www.ssa.gov/history/ssa/ssa2000chapter6.html

Social Security cards carried specific instructions "for Social Security and tax purposes—not for identification."[7]

Ⅲ. Uses of Social Security Numbers

Both private persons and government agencies use social security numbers as an identifier. Some of the uses are legally mandated, others are voluntary decisions made by those that maintain the database.

a. Financial Information

As stated before, the issuance of Social Security Numbers was originally to track benefits associated with employment and income. The most logical use of Social Security Numbers would be to track income. The connection with finances and these numbers has expanded greatly, to both governmental and private sectors.

The largest private sector usage of Social Security Numbers is by companies that learn and share financial information about Americans, specifically credit bureaus.[8] These companies, who are usually against Social Security restrictions, have large databases with information (such as name, social security number, addresses, phone numbers, occupation, gender, ethnic background, marital status, and education). This information, historically, has been sold and traded with little legal limitation.

The governmental use of Social Security Numbers is primarily for federal and state taxation of earnings. The Internal Revenue Service first began to use Social Security Numbers in 1961. This governmentally mandated usage by the Internal Revenue Code for Social Security Numbers to be the primary identification number for individuals who file tax returns and also requires Social Security Numbers to be submitted for any dependent for whom the taxpayer will claim a deduction.[9]

---

6) Id.

7) Pear, Robert, The Nation; Not for Identification Purposes (Just Kidding), N.Y. Times, July 26, 1998. http://www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html

8) Komuves, Flavio L., We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. Marshall J. Computer & Info L. 529, , 536 1997-1998.§

9) See 26 U.S.C. § 6109(d) (1994).

In 1996, the federal welfare reforms provided allowances and occasional mandatory use of Social Security Numbers as a means of locating individuals who fail to pay child support or alimony pursuant to a court order. Prior to these reforms, it was permissible for the government to use the numbers to collect money owed to the government, but the 1996 law extended the use to child support payments.[10] This new law requires a database containing the names and Social Security Numbers of all people who owe or are owed child support.[11]

For people seeking to receive a federal educational grant or loan, they must provide a Social Security Number to the school for which they are applying. This requirement helps the government to track down defaulting borrowers.[12] Universities, private and public alike, frequently use Social Security Numbers as student identifying numbers, as it is thought to better coordinate internal record keeping.[13]

b. Law Enforcement and the Legal System

In addition to using Social Security Numbers for tracking debt to both governmental and private parties, the legal system has also implemented practices which rely on this as an identification number.

The largest criminal justice database in the United States, the National Crime Information Center (NCIC) maintains a list of convicted criminals and fugitives.[14] When someone's name is entered into the interstate identification files, the Social Security Number, if available, is also included in that data. This information is not mandated to be provided by individuals, as law enforcement agencies may not request Social Security Numbers without statutory disclosure, it is often included as the number is known.

Many state maintained law enforcement also utilize the Social Security Number as an identification number. In fact, in some states, the Social Security Number or a date of birth is required when someone (anyone) seeks to obtain a copy of another person's criminal history.[15] Although requesting

10) See 42 U.S.C. § 405(c)(2)(C)(ii)(1994), See 5 CFR 581.203(a)(3)(1996)
11) See 42 U.S.C. § 653(d)(1)(West Supp. 1997)
12) See 20 U.S.C. § 1091(a)(4)(B) (1994).
13) Komuves, at 538; See also, Alexander C. Papndreou, Krebs v. Rutgers: The Potential for Disclosure of Highly Confidential Personal Information Renders Questionable the Use of Social Security Numbers as Student Identification Numbers, 20 J.C. & U.L. 79, 79 n.2 (1993).
14) See Notices- Department of Justice- Privacy Act of 1974 Modified System of Records, 60 Fed. Reg. 19774 (April 20, 1995)

a suspect's Social Security Number is not authorized by, and is most likely forbidden by Section 7 of the Privacy Act of 1974, it is often a routine request in questioning by law enforcement.[16)]

The usage of Social Security Numbers by the legal system is not limited to law enforcement, Bankruptcy and Tax Court rules require submission of Social Security Numbers by either the debtor or the preparer and the petitioner.[17)] It is also routinely requested by attorneys in civil cases for persons identified in interrogatories, though a court may still uphold a refusal to provide should the number not be calculated to lead to the discovery of evidence.[18)]

Several states also use Social Security Numbers for identification and tracking of drivers, as it is authorized by the federal government.[19)] But, there is a Congressional ban on disclosure of "personal information" on drivers' licenses, so the actual number is not attached to the form of identification.[20)]

c. Medical Purposes

A controversial use of Social Security Numbers has been the federal authorization for states and private entities that collect blood donations to collect Social Security Numbers, and for states to require furnishing the number as a condition for donating blood.[21)] This provision was enacted to determine whether donors should be excluded from donating blood because of disease, the practice has been criticized as an unforeseen invasion of privacy.[22)]

Social Security Numbers are collected and maintained by both states and also organizations such as the Medical Information Bureau, which is maintained in Massachusetts and warehouses millions of United States residents' medical records.[23)]

---

15) See NJ Stat. Ann. 53:1-20.6 (West 1986 & Supp. 1996).
16) Komuves, at 536, see also United States v. Johnson, No. 9405225, 1995 WL 88947, at 3
17) See, e.g. Fed. R. Bankr. P. 1005 ("the title of the case shall include the name [and] social security number and employer's tax identification number…"), See Tax Court R. 34(b)(1) (requiring that the petition filed with the Tax Court include "an identification number e.g., Social Security Number or employment identification number.")
18) See, e.g. In re Amendments to Rules of Civil Procedure, 577 So. 2d 580, 581 (fla. 1991) (adopting standard interrogatories in which the SSN of litigants is requested.)
19) See 42 U.S.C. §405(c)(2)(C)(i)
20) See 18 U.S.C. § 2725 (West Supp. 1997)
21) See 42 U.S.C. § 405(c)(2)(D) (1994)
22) Coleman v. American Red Cross, 23 F.3d 1091 (6th Cir. 1994)
23) See Steve A. Bibas, A Contractual Approach to Data Privacy, 17 Harv. J.L. &Pub. Policy 591, 593-95 (1994).

Ⅳ. REAL ID ACT 2005

In 2005, the Federal Government passed a law that some say would create a national identification system by connecting states' driver-licensing systems. This law was passed after the 9/11 Commission recommended federal standards for the issuance of identification, such as driver's licenses.[24)]

To comply with this law, the following elements must appear on all drivers licenses and ID cards that would be accepted for federal use:

- The person's full legal name
- The person's date of birth
- The person's gender
- The person's driver's license or personal identification card number
- A digital photograph of the person
- The person's address of principal residence
- The person's signature[25)]

In addition, the Act required that a state must include anti-counterfeit technology in its driving licenses, verify an applicant's identity and validation that the applicants are lawfully present in the United States, to prevent illegal immigrants from receiving a driver's license. and conduct background checks for employees involved in issuing driver's licenses. The standards would also allow users' information to be shared with ease in a national database.

National Identification Numbers are hard to define, the "hallmarks of a national ID," have been identified as one that is "national in scope," is "used for identification," and is "legally or practically required." [26)] Many argue that this REAL ID Act is, like Social Security Numbers, though not

---

24) National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States, 390
Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.

25) Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, 109th Cong.

26) Karrie Ann Jefferson, What's in a Name: a comparative analysis of the United States REAL ID Act and the United Kingdom's National Identity Scheme, Calhoun Naval Postgraduate School Thesis Collection, December 2015; see also, Harper, "Testimony regarding SB 262 and the US Federal Real ID Act: Committee on Transportation New Hampshire

admitting to be a national identification program, a de facto national identification number system.

The Department of Homeland Security maintains that this national set of standards is not a national identification card, as it does not create a federal database of driver license information[27]. The new identification requirements are considered as a useful tool in fighting terrorism. In addition to fighting terrorism, the other benefits are cited as: reducing identity theft, reducing unqualified driving, reducing fraudulent access to government subsidies and welfare programs, reducing illegal immigration, reducing unlawful employment, reducing unlawful access to firearms, reducing voter fraud, and possibly reducing underage drinking and smoking.[28]

As of January 8, 2016, 23 states are in full compliance with the act, 27 states and territories have been granted extensions. Six states and territories have taken no steps to comply with the controversial law.[29]

Ⅴ. Privacy Concerns with Current Systems

Even at the start of the Social Security system, the public was concerned about privacy and confidentiality. The concerns range from how the system will function, how the data will be collected, used, maintained and protected. Those that oppose national identification card systems believe that it enables the government and potentially private companies and individuals to collect and disseminate personal information.

Privacy is not an enumerated right in the United States Constitution or any amendments. The Supreme Court has held, in Griswold v. Connecticut, that "various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment," and the Third, Fourth, Fifth, and Ninth Amendments were held to give people a right to privacy. This doctrine has been used in many cases since, but there has been some debate as to whether this constitutional right to privacy also includes a right to anonymity. The concerns over national identification numbers raise this question, do United States citizens have the right to hide one's identity? Or is it merely the right to

---

State Senate."

27) https://www.dhs.gov/real-id-public-faqs

28) Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 1086 (March 9 2007).

29) Jad Mouawad, US Gives States 2 More Years to Meet Driver's License Standards, N.Y. Times, Jan 8, 2016. http://www.nytimes.com/2016/01/09/business/us-gives-states-2-more-years-to-meet-drivers-license-standards.html

control and not disseminate personal information? Once a national identification numbering system is fully implemented, requiring mandatory reporting and compelled production of that identification, the right to control that information may be out of a citizen's hands for good.

a. Data Security

Concerns about deliberate or negligent breaches that would lead to abuse are some of the more passionate arguments against a national identification system, as oversight would be massive. The Social Security Board, at the inception of Social Security Numbers, aware of these concerns, issued releases to assure assuring the public that the information on the application would be kept confidential, with access limited to government employees for whom job duties under the Social Security Act required it.[30] As far back as June 1937, the Social Security Board first issued a regulation that formalized the promise of confidentiality for information collected and maintained.

b. Function Creep

Historically, the misuse of Social Security Numbers leads many to be concerned that national identification cards could be used in ways that exceed their stated purpose. This has been referred to as a "function creep."[31] Even though there has been protection through the 1974 Privacy Act against the government using personal information, there is no such restriction on private companies or individuals. Those that oppose the REAL ID licenses cite concerns that those identity cards and unique identifiers will be used well beyond their original purpose. Some even claim that the use of driver's license in this REAL ID scheme, is itself a function creep, as driver's licenses were created only to authorize a person to operate a motor vehicle, not as an identification card for verifying age, address, or whether or not someone is a terrorist.

c. Data Integrity

With the huge breadth of this database, the accuracy, consistency and reliability of the data is

30) https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html
31) Jefferson at 43.

essential. In particular, if this data is being used to identify those involved in terrorism, mistakes could lead to disasters if the incorrect person is identified.

At this time, the Notice of Proposed Rulemaking indicates that all states will need to adopt the fair information practice principles, which are the crux of the Privacy Act of 1974 to receive DHS certification that they are fulfilling the requirements of the REAL ID Act.[32] Critics believe that these are not high enough privacy standards and that the full federal privacy standards should be applied to the states to create uniform redress standards, which are not included in the fair information practice principles.

d. Securely Linking Databases

Furthermore, the linking of Databases and expanded sharing of data poses some risk of a decrease in the overall security of the system. If someone were to wish to hack into a system, rather than having to hack into all states individually, just one would be necessary. The linking of the systems has been characterized as "more insecure than creating a large centralized database in terms of safeguarding the data."[33] [34]

The increased availability and aggregation of personal data, including Social Security numbers has exposed many to identity theft. These crimes have illustrated that aggregated personal information can be vulnerable to security breaches.

Ⅵ. Purpose Concerns With Current System

Is a national identification system necessary for the purposes for which they are created? Those who oppose the REAL ID Act and the expanded use of the Social Security numbers question whether ID cards will actually improve national security, prevent terrorism, and increase safety.

---

32) Minimum Standards for Driver's License and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10826, (March 9, 2007).

33) Jefferson, at 51.

34) http://www.gao.gov/new.items/d051016t.pdf

a. No Evidence Terrorism Will Stop

As of April 2004, the following statistics were given for assessing the impact of national identity cards: “Of the 25 countries that have been most adversely affected by terrorism since 1986, eighty per cent have national identity cards, one third of which incorporate biometrics. This research was unable to uncover any instance where the presence of an identity card system in those countries was seen as a significant deterrent to terrorist activity.”[35)]

In addition, the 9/11 terrorists were able to obtain compliant identifications fraudulently, and there is no information that shows that REAL ID compliant licenses will not be able to be obtained fraudulently as well. The use of legitimate documentation to avoid the system is known in counterterrorism as logical avoidance, this could be a preferred strategic move, as many terrorists operate under their own names already.[36)]

b. Increased Risk of Identity Theft

As noted above, the data breach concerns also give rise to an increased risk of identity theft, as linked databases are less secure and more susceptible to hacking. Plus, with the database being linked, inadvertent security breaches could have much greater consequences, again opening citizens to the possibility of identity theft due to negligence.

More Problems with Illegal Immigration and Unlawful Employment

By increasing requirements to apply for lawful driver’s licenses, some worry that this REAL ID Act will “undermine national security by pushing immigrants deeper into the shadows and forcing many to drive without licenses.”[37)]

35) Jefferson at 40, See also Mistaken Identity: Exploring the Relationship between National Identity Cards & the Prevention of Terrorism,” April 2004, http://www.privacyinternational.org/issues/idcard/uk/id-terorism.pdf

36) Id.

37) Jefferson at 41,See also Debra Milberg, “National Security Surveillance and National Authentication System: The National Identification Debate: “REAL ID” and Voter Identification.” I/S: A Journal of Law & Policy for the Information Society 3, no. 3 (Winter 2007) 443-472.

Ⅶ. Federal Protection of Social Security Numbers

a. Privacy Act of 1974

Currently, the main source of restrictions on governmental usage of Social Security Numbers comes from Section 7 of the Privacy Act of 1974.[38] The Privacy Act provides that it is unlawful for any Federal, State or local government to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number."[39]

This provision does not, however, apply to disclosures required by federal statute or any disclosure of the number to any federal, state, or local agency maintaining a system of records. This caveat is where the majority of disclosures of this supposedly secret number have occurred. It should also be noted that Section 7 does not contain any restrictions on private actors, so this act is inapplicable to private individuals or companies.

b. Exemption Six of the Freedom of Information Act

The Freedom of Information Act, commonly known as FOIA, passed in 1994, requires federal agencies to generally make their records available to the public, unless a specific exemption applies. Exemption 6, allows an agency to withhold records that would "disclose information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy." Courts have held that Social Security Numbers are to be withheld under this exemption, protecting citizens from dissemination upon request.[40]

c. Identity Theft and Assumption Deterrence act of 1998

In 1998, in order to stop the growing problem of identity theft, Congress made it a federal crime. The act made it a federal criminal offense for a person to "knowingly transfer, possess, or use without lawful authority," another person's means of identification "with the intent to commit, or to aid, abet,

38) 5 U.S.C. §552(a)(7)(a)(1)
39) Id
40) 5 U.S.C. §552(a)(1994).

or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." The Social Security Number is considered a "means of identification" and cases have been prosecuted under this law.

Ⅷ. Conclusion

Although the United States does not have a "National Identification System," the Social Security Number has served as a de facto national identification number for almost a century. With the passage of the REAL ID Act in 2005 and the reluctant compliance by most states, the path to a national identification system has been shown. But, opponents, both in state legislatures and in the academic world have major concerns regarding privacy, data mishandling, a disconnect from the stated purpose and a real potential for expanded use of any national identification database. With these concerns, the debate continues, and as evidenced by the need in the extension of the REAL ID deadline, systematic compliance is not here as of now.

미국의 개인식별번호체계에 관한 법적 쟁점

Ⅰ. 서 론

미국은 개인식별번호체계를 갖고 있지 않다. 다만, 사회보장번호는 실질적인 식별체계로 사용되고 있고 본래적으로 사회보장을 추적하기 위해 숫자상의 체계로 마련되었다. 개인의 사회보장번호는 기본적으로 일반적인 식별번호의 목적을 갖고 있다. 그러나 이것은 사회보장프로그램의 목적이 아니며 효과적인 국민 식별체계 역시 아니다.

미국정부는 오랫동안 국민식별 관리체계를 실행하기 위해 논의해왔다. 이러한 식별 프로그램에 대한 정치인과 찬성론자들은 이 체계가 테러를 방지, 신원도용으로부터 국민을 보호, 여행에 도움을 주며 합법적 고용을 감독하고 불법적인 고용과 보조금을 확인할 수 있다고 주장하고 있다.

반면, 국민식별관리체계를 반대하는 자들은 이러한 형태의 체계가 시행된다 하더라도 정부가 명시한 많은 문제들이 해결되지 않을 것이라고 주장하고 있다; 예를 들어 테러가 감소된다는 것이 그것이다. 추가적으로, 그들은 국민식별번호데이터베이스가 시행되는 경우, 일반적인 프라이버시 문제, 국민감시와 검열의 증가, 신원도용의 위험 증가라는 문제점이 발생할 것을 우려하고 있다.

본 논문은 사회보장번호체계를 시작으로 미국의 식별체계의 역사적 배경을 검토할 것이다. 즉, 식별체계가 어떻게 일반적인 식별번호에 준하여 고용과 퇴직연금을 추적할 수 있는가라는 것이다. 또한 본 논문은 2005년에 통과한 실질신원법과 운전자 면허에 관한 새로운 법이 주에 의해 시행되고 있음을 검토할 것이다. 본 저자는 사회보장번호의 현행 사용과 국민식별번호체계의 헌법성과 오용으로부터 국민을 보호하기 위해 마련된 실질신원법에 대해 법적 쟁점을 분석할 것이다. 미국은 이러한 쟁점이 나뉘어져 있는 상태이며 국민식별프로그램의 시행은 절박한 현실이 아니라는 것은 명확하다.

Ⅱ. 사회보장번호의 역사적 배경

사회보장은 1935년에 통과된 사회보장법, 즉, 뉴딜정책의 부분으로써 사회보장행정프로그램

으로 시작된 사회보험프로그램이다.[1] 사회보장번호는 이 프로그램이 시작된 후 1년뒤에 만들어진 것으로 사회보장혜택의 권한을 추적할 목적으로 시행되었다. 사회보장은 65세 또는 그 이상의 퇴직자에게 이전 소득을 근거한 계속적 수입을 보장하기 위해 만들어진 사회보험프로그램을 의미한다.[2] 점진적으로, 사회보장은 장애자, 퇴직자의 가족, 장애 또는 실업 근로자의 혜택으로 포함·확장되었다.

1936년 6월, 사회보장위원회는 9개의 숫자 체계를 결정하였다. 첫 번째 3개의 숫자는 지역번호, 다음 2개의 숫자는 그룹번호를 의미하는 것으로 우체국에서 10,000개의 그룹으로 발급된 번호로 결정되어 처음은 홀수로 시작되어, 다음은 짝수, 마지막은 홀수로 구성된다. 마지막 4개의 숫자는 일련번호로 각각의 그룹 내 0001부터 999까지 순서대로 나열되어있다.[3]

1936년에 시작된 우체국은 해당 지역의 우체부에 의해 제공된 목록을 바탕으로 사용자에게 신청서를 배포함으로써 사회보장번호를 등록하기 시작했다. 이것은 그때 당시에 약 240만 사용자들에 의해 등록되었다.[4] 2008년 12월, 사회보장행정국은 미국에 살고 있는 거의 모든 주민들에게 4억 5천개의 초기 사회보장번호를 발급하였다.

초기에는, 고용상태의 근로자들과 64세 또는 그 이하의 사람들은 사회보장번호를 받을 권리가 있었지만, 이미 사회보장에 등록된 사람들에게 우선 채용에 관한 문제가 발생한 후 , 사회보장국은 신청자에게 사회보장번호를 발급하기 시작하였다.[5]

사회보장번호카드는 전적으로 신원을 증명하지 않는다.[6] 사실상, 많은 시간 동안, 사회보장카드는 신원을 위한 것이 아니라 "사회보장과 세금 목적을 위해' 라는 특별한 지침서가 전달된 것이다.[7]

---

1) Puckett, Carolyn, The story of the Social Security Number, Social Security Bulletin, Vol. 69, No. 2, 2009. https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

2) Historical Background and Development of Social Security, https://www.ssa.gov/history/briefhistory3.html

3) Id.

4) McKinley, Charles, and Robert W. Frase. Launching Social Security: A capture-and-record account, 1935–1937. Madison, WI: The University of Wisconsin Press, 344-45 and 368, 1970.

5) History of SSA 1993 - 2000, Chapter 6: Program Integrity. Available at: http://www.ssa.gov/history/ssa/ssa2000chapter6.html

6) Id.

7) Pear, Robert, The Nation; Not for Identification Purposes (Just Kidding), N.Y. Times, July 26, 1998. http://www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html

Ⅲ. 사회보장번호의 사용영역

사인과 정부기관은 식별자로써 사회보장번호를 사용한다. 이러한 사용영역의 몇 부분은 법적으로 위임되어 있지만, 다른 것들은 데이터 베이스를 유지하는 자발적인 결정에 의하고 있다.

a. 재정정보

앞서 설명한 바와 같이, 사회보장번호의 발급은 본래적으로 고용과 소득에 관한 혜택을 추적하기 위한 것이었다. 사회보장번호의 가장 합리적 사용은 소득을 추적하기 위한 것이다. 재정과 이 번호의 연계성은 정부와 사적 영역으로 크게 확장되어왔다.

사회보장번호의 가장 큰 사적 영역의 사용은 미국인에 대한 재정정보를 습득하고 공유하는 특히, 신용 조사기관이라는 회사에 의한다. 사회보장규제에 반하는 이러한 회사들은 정보에 관한 큰 데이터베이스(이름, 사회보장번호, 주소, 전화번호, 직업, 성, 민족, 결혼상태, 교육)를 가지고 있다. 이러한 정보는 역사적으로 거의 법적 제한 없이 판매되고 거래되어 왔다.[8)]

사회보장번호의 정부 사용은 우선 연방과 주의 소득세를 위한 것이다. 국세청은 처음으로 1961년 에 사회보장번호를 사용하기 시작했다. 이것은 세금신고를 하는 개인의 우선식별번호로써 국세법은 정부로 하여금 사회보장번호의 사용을 위임하였고 납세자로 하여금 감면을 주장하는 배우자를 위하여 사회보장번호를 제출하도록 요구하였다.[9)]

1996년, 연방보장개혁은 자녀를 원조하지 못하는 개인을 찾아내는 방법으로 또는 법원의 법령에 따른 부양비로써 인적 공제와 사회보장번호의 의무적 사용을 제공하고 있다. 이러한 개혁이 있기 전, 정부는 빚진 돈(채무)을 청구하기 위해 번호를 사용하였지만, 1996년 법은 자녀지원금의 사용을 위해 그 범위를 확장하였다.[10)] 이 새로운 법은 자녀 지원을 원하는 모든 사람들의 이름과 사회보장번호를 포함한 데이터 베이스를 요구하고 있다.[11)]

연방교육보조금 또는 대출금을 받기를 원하는 사람들은 지원하는 학교에 사회보장번호를 제공하여야 한다. 이러한 사항은 정부가 채납된 대출자를 추적하는데 도움을 준다.[12)] 사립 또는 공립 대학들은 내부보존기록을 더 잘 편성할 목적과 학생을 확인할 수단으로 사회보장번호를

8) Komuves, Flavio L., We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. Marshall J. Computer & Info L. 529, , 536 1997-1998.§
9) See 26 U.S.C. § 6109(d) (1994).
10) See 42 U.S.C. § 405(c)(2)(C)(ii)(1994), See 5 CFR 581.203(a)(3)(1996)
11) See 42 U.S.C. § 653(d)(1)(West Supp. 1997)
12) See 20 U.S.C. § 1091(a)(4)(B) (1994).

사용한다.[13]

b. 법 집행과 법 체계

정부와 사적 당사자는 채무를 추적하기 위해 사회보장번호를 사용하는 것과 더불어, 사회보장번호를 식별번호로써 법 체계의 집행을 시행하고 있다.

미국의 가장 큰 형사법 데이터 베이스인 전국범죄정보센터는 범죄자와 지명수배자의 정보를 보유하고 있다.[14] 어떤 이의 이름이 주간(사이) 식별 파일에 입력되는 경우, 사회보장번호는 그 정보에 역시 포함되어 있다. 이 정보는 법적인 승인 없이, 법 집행기관들이 사회보장번호를 요구하지 않는 것처럼 개인에 의해 제공되고 있다.

많은 주들은 법 집행 역시 식별번호로써 사회보장번호를 이용하고 있다. 사실상, 몇몇 주 내에, 사회보장번호 또는 생년월일은 개인이 다른 사람의 범죄 기록 사본을 발급받고자 하는 경우, 요구 되어진다.[15] 피의자의 사회보장번호를 요구하는 것이 1974년 프라이버시 법 제7조에 의거 권한이 없거나 금지된다 하더라도, 이것은 법 집행에 의한 일반적인 심문절차이다.[16]

법 체계에 따른 사회보장번호의 사용은 파산과 조세법원 규정이 채무자, 대리인, 그리고 청원인에게 사회보장번호를 제출할 것을 요구하는 것과 같은 법 집행에 제한을 두지 않는다.[17] 법원은 사회보장번호가 증거발견의 단서로써 판단되지 않아 제공을 거절하는 경우가 있다 할지라도 사회보장번호는 일반적으로 심문조서에 확인이 되는 사람에 대해 민사사건 변호사가 역시 요청할 수 있다.[18]

여러 주들은 역시 연방정부의 권한을 부여 받으므로써 운전자의 식별 및 추적을 위해 사회보장번호를 사용한다.[19] 그러나 운전자 면허의 개인정보를 공개하는 것을 의회는 금지하고 있어, 실질적 번호는 식별형태로 첨부되지 않는다.[20]

---

13) Komuves, at 538; See also, Alexander C. Papndreou, Krebs v. Rutgers: The Potential for Disclosure of Highly Confidential Personal Information Renders Questionable the Use of Social Security Numbers as Student Identification Numbers, 20 J.C. & U.L. 79, 79 n.2 (1993).

14) See Notices- Department of Justice- Privacy Act of 1974 Modified System of Records, 60 Fed. Reg. 19774 (April 20, 1995)

15) See NJ Stat. Ann. 53:1-20.6 (West 1986 & Supp. 1996).

16) Komuves, at 536, see also United States v. Johnson, No. 9405225, 1995 WL 88947, at 3

17) See, e.g. Fed. R. Bankr. P. 1005 (“the title of the case shall include the name [and] social security number and employer’s tax identification number…”), See Tax Court R. 34(b)(1) (requiring that the petition filed with the Tax Court include “an identification number e.g., Social Security Number or employment identification number.”)

18) See, e.g. In re Amendments to Rules of Civil Procedure, 577 So. 2d 580, 581 (fla. 1991) (adopting standard interrogatories in which the SSN of litigants is requested.)

19) See 42 U.S.C. §405(c)(2)(C)(i)

c. 의료목적

사회보장번호의 사용이 논란이 되는 것은 사회보장번호를 수집하기 위해 헌혈증서를 모으는 주와 개별기관 그리고 헌혈의 조건으로써 사회보장번호를 요청하는 주에게 연방이 권한을 부여하고 있다는 것이다.[21] 이 규정은 기부자가 헌혈을 제공한다 할지라도 질병으로 인해 이를 배제할 수 있는지를 결정하기 위해 마련되었다. 따라서 이러한 행위는 예상치 못한 프라이버시 침해로써 비판 받고 있다.[22]

사회보장번호는 주와 의료정보국과 같은 기관에 의해 수집되고 유지·관리되며 메사추세츠와 수백만 미국 주민의 의료기록 데이터 베이스를 유지 관리하고 있다.[23]

Ⅳ. REAL ID ACT 2005(2005년 실질신원법)

2005년, 연방정부는 주의 운전자면허 시스템을 연결함으로써 국민식별체계를 만들 수 있는 법을 통과시켰다. 이 법은 9/11 위원회가 운전자 면허와 같은 식별확인을 위해 연방 기준안을 권고한 후 통과되었다.[24]

이 법에 따라, 다음의 사항들은 연방사용을 위해 인정되는 운전면허증과 신원카드에 기재되어야 한다:

- (본인) 법적 성명
- 생년월일
- 성별
- 운전자 면허번호와 신원확인카드 번호

---

20) See 18 U.S.C. § 2725 (West Supp. 1997)

21) See 42 U.S.C. § 405(c)(2)(D) (1994)

22) Coleman v. American Red Cross, 23 F.3d 1091 (6th Cir. 1994)

23) See Steve A. Bibas, A Contractual Approach to Data Privacy, 17 Harv. J.L. &Pub. Policy 591, 593-95 (1994).

24) National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States, 390
Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.

- 디지털 사진
- 주거지의 주소
- 서명[25]

추가적으로, 이 법은 해당 주로 하여금 운전면허증에 대한 위조방지기술을 포함해야 하고, 운전자 면허를 소지함으로써 불법이민을 방지하기 위해 신청자의 신원과 신청자가 법적으로 미국에 거주하고 있다는 합법성을 확인하며, 운전자의 면허를 발급함에 있어 근로자의 신원조회를 수행해야 한다고 요구하고 있다. 이러한 기준은 사용자의 정보로 하여금 국가 데이터베이스에 쉽게 접근·공유할 수 있도록 해준다.

국민식별번호는 범위 내 국민을 식별하기 위해 사용되어 지는 경우, "국민신원의 특징" 과 "법적으로 또는 실무상 요구되는" 이라고 정의하기가 어렵다.[26] 많은 사람들은 실질신원법이 국민식별프로그램 즉, 실질적인 국민식별번호 체계로 받아들여지지 않는다 할지라도 실질신원법이 사회보장번호와 유사하다고 주장하고 있다.

국토안보부는 국가전체의 기준이 운전자 면허 정보의 연방 데이터베이스를 만들지 않았던 것처럼 그 기준이 국민식별카드가 아니다라고 주장하고 있다.[27] 새로운 식별 사항들은 테러를 방지하기 위한 유용한 수단으로써 인식되고 있다. 테러를 방지하는 것과 더불어, 다음과 같은 다른 유용한 점들이 있다: 신원도용의 감소, 무자격 운전의 감소, 정부보조금과 복지 프로그램에 대한 사기적 접근 감소, 불법이민의 감소, 불법고용의 감소, 총기의 불법적 접근 감소, 투표사기를 감소, 미성년자의 음주와 흡연의 감소.[28]

2016년 1월 8일, 23개의 주들은 이 법을 전면적으로 준수할 것을 천명한 반면, 27개의 주와 구역들은 연기신청을 하였다. 그 외6개 주와 구역들은 논란이 되고 있는 법에 대해 어떠한 조치를 취하지 않고 있다.[29]

---

25) Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, 109th Cong.

26) Karrie Ann Jefferson, What's in a Name: a comparative analysis of the United States REAL ID Act and the United Kingdom's National Identity Scheme, Calhoun Naval Postgraduate School Thesis Collection, December 2015; see also, Harper, "Testimony regarding SB 262 and the US Federal Real ID Act: Committee on Transportation New Hampshire State Senate."

27) https://www.dhs.gov/real-id-public-faqs

28) Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 1086 (March 9 2007).

29) Jad Mouawad, US Gives States 2 More Years to Meet Driver's License Standards, N.Y. Times, Jan 8, 2016. http://www.nytimes.com/2016/01/09/business/us-gives-states-2-more-years-to-meet-drivers-license-standards.html

Ⅴ. 현행 체계의 프라이버시 문제

사회보장체계가 시작되는 시점에, 사람들은 프라이버시와 보안(안전)에 대해 걱정을 토로했다. 이러한 문제는 이 체계가 어떻게 기능할 것이며, 그러한 정보가 어떻게 수집, 사용, 유지, 보호될 것인지에 대해 연관이 있을 것이다. 국민식별카드체계를 반대하는 사람들은 이 체계가 정부와 사기업, 개인에게 개인정보를 수집하고 배포할 수 있다고 생각한다.

프라이버시는 미국헌법상 또는 수정헌법에 규정된 권리는 아니다. Griswold v. Connecticut 사건에서, 대법원은 "다양한 약속들이 프라이버시 영역을 만든다"라고 판결하였다. 단결할 권리는 첫 번째 수정헌법상에 규정되어 있으며 세 번째, 네 번째, 다섯 번째, 그리고 7번째 수정헌법은 사람들에게 프라이버시 권리를 부여하고 있다. 이 원칙은 그 이후 많은 사례에서 사용되고 있으나 프라이버시라는 헌법상의 권리가 역시 익명성을 포함하고 있는지에 대한 논란이 있다. 국민식별번호에 대한 문제는 미국 시민들이 개인의 신원을 숨길 권리를 가지고 있는가라는 질문을 제기하고 있다. 또는 프라이버시 권리는 단지 개인정보를 감독하고 배포하지 않을 권리를 의미하는 것인가? 국민식별번호체계가 전적으로 시행되자 마자, 정보를 감독할 권리 즉 의무적 보고와 강제적 식별성은 선의상 시민들의 손을 벗어나고 있다.

a. 정보 안전(보호)

권리 남용과 같은 고의 또는 과실 위반에 대한 문제는 국민식별체계에 대하여 격렬한 논쟁이 되고 있다. 사회보장위원회는 사회보장번호의 인식에 있어 이러한 문제를 주지하고 있으며 사회보장법에 따라 정부근로자들은 정보를 제한적으로 접근해야 하며 더불어 정보를 적용함에 있어 비밀성(보안)을 유지할 것이다라는 사실을 대중에게 확신시킬 수 있도록 해야 할 것이다.[30] 1937년 6월, 사회보장위원회는 처음으로 정보수집과 유지에 대해 비밀성을 약속하는 규정을 발표하였다.

b. Function Creep (사적 정보 유출)

역사적으로, 사회보장번호의 오용은 많은 사람들에게 국민식별카드는 그 목적을 넘어서는 방법으로 사용될 수 있다는 문제점을 제기하고 있다. 이것을 사적 정보 유출이라고 지칭한다.[31]

30) https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html
31) Jefferson at 43.

1974년 프라이버시 법은 개인 정보를 사용하는 정부에 반하여 정보를 보호한다 할지라도 사기업과 개인에 대한 제한은 없다. 실질신원면허를 반대하는 자들은 신원카드와 특수한 신원 식별자들은 본래적 목적을 벗어나 사용될 수 있다는 것을 주장하고 있다. 반대론자 중 몇몇은 심지어 운전자 면허가 나이, 주소를 확인하기 위한 식별 카드가 아닌 또는 어떤 이가 테러리스트인지 여부를 확인하는 것이 아닌 단지 자동차를 운전하기 위해 개인에게 부여되는 것으로 발급됨에 따라 실질신원체계상 운전자 면허의 사용은 그 자체로 사적 정보 유출이라고 주장하고 있다.

c. 정보 완전성

이러한 데이터 베이스의 광대한 양으로 인해, 정보의 정확성, 일관성, 신뢰성은 필수적인 것이다. 특히, 정보가 테러와 관련된 사람들을 확인하기 위해 사용되는 경우, 잘못된 사람을 확인한다면, 그 실수(오류)는 참담한 재앙이 될 수 있다.

이 시점에, 제안된 규칙제정의 지침(권고지침)은 모든 주는 공정한 정보실행원칙, (즉 실질신원법의 요구사항을 수행하고 있다는 DHS증명서를 받기 위해 1974년 프라이버시 법의 중요한 부분)을 채택해야 한다고 지적하고 있다.[32] 비판론자들은 이것이 프라이버시 기준으로 충분하지 않고 연방 프라이버시 기준들은 획일적인 보상기준을 만들기 위해 해당 주에 적용되어야 하는 것으로 공정한 정보실행원칙에 포함되지 않는다고 생각한다.

d. 데이터베이스의 안전한 접근(안전한 정보접근)

더욱이, 데이터베이스의 접근과 정보의 확장적 공유는 체계 전체의 안전을 감소시킬 수 있는 위험성을 발생시킨다. 어떤 이가 각 주를 개별적으로 해킹하기 보다 이러한 체계를 해킹하고자 하는 경우, 단 한가지가 필요할 것이다. 체계의 접근은 “정보를 안전하게 지킴으로써 중앙집중 데이터베이스를 만들기 보다 좀 더 불안전한” 특징을 갖고 있다.[33][34]

사회보장번호를 포함한 개인정보 이용성의 증가와 공격은 신원도용에 노출되어 있다. 이러한 범죄는 총합된 개인정보가 안전위반에 취약할 수 있다는 것을 설명하고 있다.

---

32) Minimum Standards for Driver’s License and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10826, (March 9, 2007).

33) Jefferson, at 51.

34) http://www.gao.gov/new.items/d051016t.pdf

Ⅵ. 현행체계의 목적성에 관한 문제

국민식별체계는 제정목적상 필요한 것인가? 실질신원법을 반대하는 자들과 사회보장번호의 확장적 사용은 신원카드가 실질적으로 국민안전을 도모하고, 테러를 방지하며 안전을 증가시킬 수 있는지 의문을 제기하고 있다.

a. 테러가 중단될 것이다'라는 증거가 없음

2004년 4월, 다음과 같은 통계는 국민신원카드의 영향력을 평가하고 있다: "1986년 이후, 테러에 의해 가장 악영향을 받은 25개의 나라 중, 8%는 국민신원카드를 시행하고 있고 그 중 1/3은 통합된 생체인식을 가지고 있다. 이 조사는 어떠한 예 즉, 신원카드체계의 시행은 테러 활동을 중단할 수 있는 중요한 방지책으로써 인식될 수는 없을 것이다.[35]

추가적으로, 9/11 테러리스트들은 위조된 승인신원을 얻을 수 있었고 승인된 실질신원 면허는 마찬가지로 위조된 것을 얻을 수 없다라는 것을 보여주는 어떠한 정보도 없었다. 합법적 서류의 사용은 테러를 방지할 수 있는 것으로 알려졌으며 이것은 많은 테러리스트들이 이미 그 자신의 이름을 가지고 실행할 경우, 전략적 포석(방지책)이 될 수 있다.[36]

b. 신원도용의 위험성 증가

위에서 설명 바와 같이, 정보위반문제는 역시 연결데이터가 덜 안전하고 해킹에 더 취약한 것처럼 신원도용의 위험성을 증가시킨다. 연결된 데이터베이스와 함께, 의도치 않은 안전위반은 과실로 인해 신원도용의 가능성을 열어 놓을 수 있는 더 큰 결과를 낳을 수 있다.

c. 불법인민과 불법고용 등의 문제

합법적인 운전자 면허를 신청하기 위해 필요한 사항들이 증가 함에 따라, 실질신원법은 "이민자들로 하여금 더 깊이 숨어들게 하고 면허 없이 운전하게 함으로써 국가안전을 침해할 것이다"라고 우려를 나타냈다.[37]

---

35) Jefferson at 40, See also Mistaken Identity: Exploring the Relationship between National Identity Cards & the Prevention of Terrorism," April 2004, http://www.privacyinternational.org/issues/idcard/uk/id-terorism.pdf

36) Id.

37) Jefferson at 41,See also Debra Milberg, "National Security Surveillance and National Authentication System: The National

Ⅶ. 사회보장번호에 관한 연방의 보호방안

a. The Privacy Act of 1974 (1974년 제정된 프라이버시 법)

최근, 사회보장번호의 정부사용에 대한 제한의 주요 법적근거는 1974년 프라이버시법 제7조이다.[38] 프라이버시법은 "개인이 사회보장번호의 공개 거절하였기 때문에 연방, 주, 또는 지방정부가 법으로 인정하는 개인권리, 혜택, 또는 특권을 부정하는 것은 불법임을 규정하고 있다."[39]

그러나 이 규정은 연방법률에 의해 요구되는 공개는 적용되지 않거나 기록체계를 유지·관리하고 있는 연방, 주, 지방기관의 번호공개에는 적용되지 않는다. 이러한 절차적 통고는 비밀번호의 공개가 이뤄지는 곳이다. 제7조는 사적 영역에서는 어떠한 제한을 포함하지 않는다. 따라서 동조는 사인 또는 사기업에 적용이 불가능하다.

b. Exemption Six of the Freedom of Information Act(정보의 자유에 관한 법 면제 6)

정보의 자유에 관한 법은 FOIA로 알려져 있으며 1994년에 통과·규정된 법으로 특별면제 규정이 적용되지 않는 경우, 국민이 이용 가능한 기록을 연방기관에게 요구할 수 있는 법이다. 면제 6은 기관으로 하여금 명확히 부당한 개인 프라이버시 침해상태에서 공개 가능한 개인정보 기록을 거부할 수 있는 규정이다. 법원은 이러한 면제 규정하에 사회보장번호를 요청이 있는 경우, 배포로부터 시민을 보호하기 위해 공개거부가 가능하다고 판시하였다.[40]

c. Identity Theft and Assumption Deterrence act of 1998(1998년에 제정된 신원도용과 추정 억제법)

1998년, 신원도용의 문제점을 막기 위해, 국회는 신원도용이 연방범죄라고 규정하였다. 이 법은 "법적 권한 없이 고의로 다른 사람의 신원을 양도, 소지, 또는 사용할 목적으로" 연방법을 위반하는 또는 "주법상 중 범죄를 구성하는 불법행위를 저지를 고의, 원조, 교사하는" 신원도용을 연방 범죄로 규정하였다. 사회보장번호는 식별방법으로 인식되고 있으며 사례들이 이

Identification Debate: "REAL ID" and Voter Identification." I/S: A Journal of Law & Policy for the Information Society 3, no. 3 (Winter 2007) 443-472.

38) 5 U.S.C. §552(a)(7)(a)(1)

39) Id

40) 5 U.S.C. §552(a)(1994).

법에 의해 기소되고 있다.

Ⅷ. 결 론

미국이 국민식별체계를 가지고 있지 않다 할지라도, 사회보장번호는 거의 1세기 동안 실질적인 국민식별번호로써 역할을 해 왔다. 2005년 실질신원법이 통과되고 대부분의 주에 의해 채택됨으로써, 국민식별체계의 길이 보이게 되었다. 그러나 주 입법부와 학문세계의 반대론자들은 프라이버시, 정보오용, 목적차단, 국민식별데이터베이스의 폭 넓은 사용의 문제점을 우려하고 있다. 이러한 우려에 따라, 논쟁이 계속되고 있고 실질신원기간을 연장할 필요성이 있다는 판단아래 체계적 준수는 현재로서 타당하지 않을 것이다.

Session 2-2

대만의 개인식별번호법제 현황과 문제점

翁清坤 | 輔仁大學財經法律學系 교수

Legal issues regarding Taiwanese Individual Identifiable Numbering System

Ⅰ. Introduction

As a tremendous amount of personal information is collected, processed, used or shared during people's daily activities, individuals' information privacy is highly risky, especially in the age of cyberspace.[1] Eugene Volokh defines the right to information privacy as "my right to control your communication of personally identifiable information about me."[2]

Right to information privacy is a subcategory of the right to privacy.[3] In fact, according to Jerry Kang, the term "privacy" embodies many concepts which can be categorized in three groups. The first group concerns "physical space," the extent to which a person's territorial solitude is protected from invaders. This spatial privacy involves the discussion of private versus public territories. The second group concerns a person's freedom to make self-defining decisions without state interference. This "decisional privacy" has provoked most contentious political and constitutional battles.[4] The third group concerns the dissemination of personal information. This "information privacy" is about an individual's control over the collection, use, and sharing of personal information.[5]

The Social Security number in the U.S. or the Identification Card Number in Taiwan is one type of personal information which is identifiable to an individual. In Taiwan, each citizen will be assigned a National Identification Card Number upon birth or naturalization registration by a household

---

1) See Susan E. Gindin, Lost and Found in Cyberspace: Information Privacy in the Age of the Internet, 34 San Diego L. Rev. 1153 (1997).

2) See Eugene Volkh, Cyberspace and Privacy: A New Legal Paradigm? Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1073-74 (May 2000).

3) See Vera Bergelson, It's Personal But Is It Mine? Toward Property Rights in Personal Information, 37 U.C. Davis L. Rev. 400-401 (December, 2003).

4) Decisional privacy is the sort discussed famously in Roe v. Wade, 410 U.S. 113 (1973). In Eisenstadt v. Baird, 405 U.S. 438, 453 (1972), the holding is that the right to privacy includes the right to decide whether or not to bear or beget a child. In Griswold v. Connecticut 381 U.S. 479, 485-86 (1965), the holding is that a law prohibiting the use of contraceptives unconstitutionally intrudes on the right of marital privacy. See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1202-1203 (1998).

5) See id.

registration office. No two persons normally possess the same number, so the potential confusion that might occur if to use names and dates of birth can be avoided. Each citizen will be uniquely identified by a numeral. Therefore, data collection would begin at birth and end at death so that each newborn as a data point will be tracked from cradle to grave through a government-issued number. The disclosure of the National Identification Card Number becomes a critical necessity to engage in a wide range of daily activities in modern society. In particular, the existence and use of a common identifier is virtually indispensable in allowing public or private organizations to differentiate one individual from another. As a result, the collection practice of National Identification Card Numbers and other personal information spans the gamut of organizations, from government agencies to non-profits, employers to financial services institutions, schools to hospitals, as well as credit card companies, retailers, websites, and many others so that they aggregate such information to establish databanks or databases.

Although a person cannot function normally without a National Identification Card Number, it is also impossible for a person to function if his or her personally identifiable information, including National Identification Card Number, is widely disseminated to others, creating the opportunity for invasion of privacy. In particular, by using the National Identification Card Number, government agencies and private industries can effectively collect, combine, and aggregate personal information from various databases. These data would paint a detailed portrait of each individual's habits and preference even though such collections would not be fully accurate or updated. In this connection, what National Identification Card Numbers do is to centralize power, and in a time when knowledge is power, then centralized information is centralized power[6].

As a consequence, due to the advent and prosperity of information economy,[7] the demand for and dissemination of personal information vastly increases. Information privacy has become a scarce commodity, especially in cyberspace. Thus, it is very important to find ways to balance information privacy and demands for personal information, including National Identification Card Numbers.

6) See Richard Sobel, THE DEGRADATION OF POLITICAL IDENTITY UNDER A NATIONAL IDENTIFICATION SYSTEM, 8 B.U. J. Sci. & Tech. L. 37, 65 (Winter 2002).

7) See Fred H. Cate, Data Protection Law and the European Union's Directive: The Challenge for the United States: The EU Data Protection Directive, Information Privacy, and the Public Interest, 80 Iowa L. Rev. 439 (March, 1995).

Ⅱ. The Development of Laws and Regulations to Protect Personal Information in Taiwan

1. Information Privacy

As in the U.S. Constitution, the term "privacy" is not explicitly incorporated into the Constitution of the ROC (Taiwan). According to Article 12 of the Constitution, "the people shall have freedom of confidentiality of correspondence." Thus, publicizing someone's letter will be explained as an infringement on her privacy. In addition, according to Article 10 of the Constitution, "the people shall have freedom of residence and of change of residence." Thus, someone's residence place shall be prevented from illegal intrusion.[8)]

Moreover, like its U.S. counterpart, the Ninth Amendment,[9)] Article 22 of the ROC Constitution states: "All other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution." The right to privacy was first explicitly addressed by the Council of Grand Justices in 1992 in its "Interpretation of Council of Grand Justice No.293 on Disputes Concerning Debtors' Rights." However, the Grand Justices failed to clarify the nature of the right to privacy. Is it a right protected by Paragraph 2 of Article 48 of Banking Law[10)] or a constitutional fundamental right under Article 22 of the Constitution? In the dissenting opinions, three Grand Justices view the right to privacy as a subcategory of personality right, which is not only a right protected by the Civil Code but also a fundamental civil right protected by the Constitution.[11)]

The interpretation of Council of Grand Justices No.293, including dissenting opinions, fails to further explain the content of privacy. Information privacy shall be seen as one of the types of the right to privacy[12)] due to Interpretation No.293 involving the protection of customer personal information under the Banking Law. Moreover, the right to information privacy also means the right to control the

---

8) See Ying-Fu You, News Media and Press, in Modern State and Constitutional Law, 769-770 (Angle Publishing Co. Ltd., Taipei, March, 1997).

9) The Ninth Amendment of the U.S. Constitution states: "The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."

10) According to Paragraph 2 of Article 48 of the Taiwanese Banking Law, a bank shall keep in confidence all information relating to customer deposits, loans and remittances unless otherwise provided by laws and regulations.

11) See generally Tzu-Yi Lin, Ji Yin ZiXun Yu Ji Yin Yin Si Quan (Genetic Information and Right to Genetic Privacy), in Dang Dai Gong Fa Xin Lun (New Theory of Contemporary Public Law), Second Volume, 697-703 (Angle Publishing Co. Ltd., Taipei, July, 2002).

12) See id.

collection, use and sharing of personal information.

The right to information privacy was first explicitly addressed by the Council of Grand Justices in 2005 in its "Interpretation of Council of Grand Justice No.603 on Disputes Concerning "the new ROC identity card not issued without the applicant being fingerprinted." The Council of Grand Justices held, information privacy is intended "to guarantee that the people have the right to decide whether or not to disclose their personal information, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed. It is also designed to guarantee that the people have the right to know and control how their personal information will be used, as well as the right to correct any inaccurate entries contained in their information."

2. What Is Personal Information?

As noted above, the right to information privacy is defined as the right to control the collection, use, and sharing of personal information. Thus, the core of the right to information privacy is to define "personal information." Personal information is defined as "information identifiable to the individual," according to the "Principles for Providing and Using Personal Information" created by the Clinton Administration's Information Infrastructure Task Force.[13)]

This definition of personal information has been interpreted to "describe a relationship between the information and a person" and to bear "(1) an authorship relation to the individual, (2) a descriptive relation to the individual, or (3) an instrumental mapping relation to the individual."[14)] First, an authorship relationship links the individual to the information prepared by the individual to communicate to someone; therefore, emails or letters constitute personal information. Second, personal information describes the biological or social status of the individual: gender, height, weight, blood type, DNA, birth date, marital status, credit history, or membership in religious or political groups. Third, one's Social Security number or ID Card number is the best example, in which case personal information is instrumentally mapped to the individual. The number is mapped to the individual by the government for recordkeeping purposes.[15)] Furthermore, personal information includes not only

13) See Henry M. Cooper, The Electronic Communications Privacy Act: Does The Answer to The Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis, 20 J. Marshall J. Computer & Info. L. 3 (Fall, 2001).

14) See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1207 (1998).

textual information, but also photographs, audiovisual images, and sound recordings of an identified or identifiable individual, whether dead or alive.[16)]

As the right to information privacy prevents only illegal collection, use, and sharing of personal information, non-personal information is left unprotected.[17)] In general, non-personal information consists of non-human information, anonymous information, and group information. Non-human information is information not connected a human being. Some anonymous materials will be seen as non-personal information. However, it is notable that anonymous information should be classified as personal information, in cases in which an individual's identity can be uncovered through publicity or research. Group information is considered non-personal information when the information is identifiable to a group of persons instead of a specific individual.[18)]

In Taiwan, the definition of personal information is similar to the theory above. Personal information means that the name, date of birth, identification card (I.D. Card) number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities of a natural person as well as other information sufficient to identify the said specific person, and other information which may be used to, directly or indirectly, identify a natural person, pursuant to Section 1 of Paragraph 1 of Article 2 of the Personal Information Protection Act.

The definition of personal information hereof is a basic one, subject to other applicable laws and regulations. For example, personal information of customers is categorized as basic information as well as account balance, credit, investment, and insurance information under the Financial Holding Company Act. As a matter of fact, disparate statutes directed at specific industries tend to differently define personal information basing on varying purposes.

---

15) See id. at 1207-1208.

16) See Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 Ind. L. Rev. 182 (1999).

17) See Henry M. Cooper, The Electronic Communications Privacy Act: Does The Answer to The Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis, 20 J. Marshall J. Computer & Info. L. 3 (Fall, 2001).

18) See id. at 3-4.

3. Market for Personal Information and Market Failures

There is also a lively market for personal information in Taiwan due to the advent and prosperity of information economy. Personal information is widely seen as a commercial asset, used both for internal marketing purposes and sale to third parties. The incentive for companies to collect, use or share personal information is very strong. Currently, industries can legally collect, use or disseminate the personal information with consent of customers. Meanwhile, there is also an illegal but widespread market for personal information, in which case criminal information collectors tend to steal personal information from government agencies or non-government institutions, such as financial institutions, telecommunication companies, and make profits by selling millions of entries of personal information to telemarketing companies or fraud gangs.[19)]

Furthermore, market failures also exist in the Taiwanese market for personal information as a result of externalities, high transaction costs, severe information asymmetries, and no privacy price discrimination. To overcome the market failures, Taiwan chooses to adopt regulatory approach, whereas the U.S. relies more on market-based mechanism. However, in the past two decades the Taiwanese Computer-Processed Personal Data Protection Law (CPPDPL), a relatively comprehensive legislation enacted in August 1995, only applied to the personal information collected, used or transferred by twelve specific sectors of private industries.[20)] In this connection, the personal information collected, used or shared by individuals and industries outside the twelve sectors would not be governed and protected by the CPPDPL; thus, most of personal information in the Taiwanese market was unregulated. Moreover, individuals or industries outside the twelve sectors could freely collect, use or share personal information unless otherwise prohibited by the Civil Code or the Criminal Code. In other words, the market for personal information facilitated by individuals or industries outside the twelve sectors could be viewed as a laissez-faire market. Nevertheless, the invisible hand concept of Adam Smith's laissez-faire theory would not be an achievable reality in the information privacy realm.[21)] This was perhaps most clearly illustrated by the fact that consumer personal information was widely collected and misused by fraud gangs all over Taiwan.[22)] As a result,

19) See Yu-Ming Chang, Wu Bai Wan Bi Ge Ren Zi Liao Bei Dao Mai (Five Million Entries of Personal Information Are Illegally Sold), Taiwan Daily, April 28, 2004.

20) CPPDPL, para. 1.6 of article 3.

21) See Jeanette Teh, Privacy Wars in Cyberspace: An Examination of the Legal and Business Tensions in Information Privacy, 4 Yale Symp. L. & Tech. 10 (2001/2002).

information privacy had become a scarce commodity. A survey from American Express Company showed that seventy-five percent of Taiwanese worried about the misuse of their personal informatio n.[23] Another survey showed that fifty-three percent of credit card holders in Taiwan lacked confidence in the bank's ability to protect customer personal information.[24] Thus, some privacy advocates required further government intervention by call for the legislature to enact stricter and more comprehensive statutes, such as the Personal Information Protection Act, to effectively protect personal information.[25] As a result, the Personal Information Protection Act was passed in 2010 and becomes effective since 2012.

4. Regulatory Approach to Protecting Personal Information

In addition to the Constitution, the following are substantial government regulations for protecting personal information in Taiwan.

A. Privacy Provisions of the Civil Code

Information privacy is one type of the right to privacy, and the right to privacy is a subcategory of the personality right. Thus, torts provisions for protecting personality rights under the Civil Code shall subsequently apply to information privacy. According to Paragraphs 1 and 2 of Article 18 of the Civil Code, when an individual's personality right is infringed upon, he or she may apply to the court to remove or prevent such infringement. Moreover, according to Paragraph 1 of Article 184 of the Civil Code, "a person who, intentionally or negligently, has wrongfully damaged the rights of another is bound to compensate him or her for any injury arising therefrom." Although the statutory language is broad and vague, the protected rights stipulated in Article 184 shall include the personality right.[26] In

22) See Zi-Hsien Chen, Dao Mai Ge ZiBei Su (Being Sued as a result of illegally selling personal information.), Chinatimes Daily, December 22, 2004.

23) See Ti Su, Wang Lu Xin Lai Biao Zhang Dui Xiao FeiZhe Xing Wei Zhi Ying Xiang (The Influence of Internet Trust Mark on Consumer's Behavior), Electronic Commerce Pilot 2 (July 15, 2004), available at http://www.ec.org.tw/Htmlupload/6-10.pdf (last visited April 16, 2016).

24) See id.

25) See Yi-Ming Lin, Bao Hu Ge Zi Jian Chi Zui Shao Yuan Ze (Personal Information Protection Requires Minimum Principle), Lihbao Daily, June 9, 2004, at http://publish.lihpao.com/2004/06/09/ (last visited May 22, 2016).

26) See Ying-Fu You, News Media and Press, in Modern State and Constitutional Law, 773 (Angle Publishing Co. Ltd., Taipei, March, 1997).

1999, the term "privacy" was added to the text of the Civil Code for the first time. The amended Paragraph 1 of Article 195 of the Civil Code stipulates that, in a case of severe wrongful injury to the body, health, reputation, liberty, creditability, "privacy," chastity, or other personality interest, the injured individual may claim a reasonable monetary compensation even if there is no pecuniary loss. As a result, an individual may claim compensation from an information collector who infringes upon her information privacy for the collector's violation of the torts provisions of the Civil Code.

B. Privacy Provisions of the Criminal Code

Article 317 of the Criminal Code states that "a person who is required by law or contract to preserve the commercial and industrial secrets of another which he knows or possesses due to his or her business and who discloses such secrets without reason shall be punished with imprisonment for not more than one year, detention, or a fine of not more than 1,000 Yuan (dollars)." Further, Article 318-1 of the Criminal Code states that "a person who discloses without reason the secrets of another which he knows or possesses by computer or other relevant equipments shall be punished with imprisonment for not more than two years, detention, or a fine of not more than 5000 Yuan." Both Articles can apply to information collectors who illegally disclose consumers' nonpublic personal information.

C. The Personal Information Protection Act

Currently, the Personal Information Protection Act, which governs the collection, use, and transfer of personal information by government agencies and private industries, is a broad and comprehensive legislation protecting personal information. However, this Taiwanese statute is different from most other models in Europe which create a single privacy commissioner. A variety of professional institutions directed at specific industries are responsible for enforcing the Personal Information Protection Act even though all of these institutions perform under the umbrella of the Ministry of Justice.[27)]

By reviewing with the OECD eight privacy principles,[28)] the followings are the substantial

27) See Fred Chilton ET AL., 1996 Computer and Telecommunications Law Update New Developments: Asia Pacific, 15 J. Marshall J. Computer & Info. L. 125 (Fall, 1996).

28) The Organization for Economic Cooperation and Development (OECD) has addressed collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. See Jody R. Westby, American Bar Association, International Guide to Privacy 84-85 (2004).

provisions of the Personal Information Protection Act:

(1) Collection Limitation Principle

Personal information shall not be collected without consent of the concerned individual, pursuant to Section 2 of Paragraph 1 of Article 15 and Section 5 of Paragraph 1 of Article 19 of the Personal Information Protection Act. In addition, Articles 8 and 9 of the Personal Information Protection Act explicitly obligate the government agencies and private industries to provide adequate knowledge to individuals about the purposes for what and how personal information is to be collected, used or shared. Therefore, the government agencies and private industries shall explain to the concerned individual the purposes of collection, use or sharing of personal information in order to obtain the required consent, by providing a clear and sufficient notice to the individual.

(2) Data Quality Principle

Personal information collected shall be relevant to the purpose for which they are to be used, pursuant to Articles 15 and 19 of the Personal Information Protection Act. Information collectors shall maintain the accuracy of personal information and make corrections or supplements thereto in accordance with their duties or at the request of the concerned individual, pursuant to Paragraph 1 of Article 11 of the Personal Information Protection Act.

(3) Purpose Specification Principle

The purpose for which personal information is collected, used or disclosed shall be specific, pursuant to Articles 15 and 19 of the Personal Information Protection Act. The Ministry of Justice shall, in conjunction with the central competent authorities in charge of the subject industries, prescribe the categories of specific purposes and the classifications of personal information, pursuant to Article 53 of the Personal Information Protection Act. However, where the scope of a specific purpose is defined more broadly, information collectors will have more freedom to collect, use or disclose personal information, and the concerned individual will receive more limitations on the rights and interests in their personal information.[29)]

29) See Wen-yi Hsu, Ge Ren Zi Liao Bao Hu Fa Lun (On Personal Information Protection) 184 (Sanmin Publishing Co. Ltd.,

(4) Use Limitation Principle

Personal information shall be used in compliance with the specific purpose of original collection unless otherwise provided by laws or agreed by the concerned individual, pursuant to Articles 16 and 20 of the Personal Information Protection Act.

(5) Security Safeguards Principle

Information collectors shall have specific security safeguard plans to prevent personal information collected from being stolen, altered without authorization, damaged, lost or disclosed, pursuant to Articles 6, 18 and 27 of the Personal Information Protection Act. Furthermore, the information collectors, the government agency or the non-government agency, shall take proper technical or organizational measures for the purpose of preventing personal information from being stolen, altered, damaged, destroyed or disclosed, pursuant to Article 12 of the Enforcement Rules of the Personal Information Protection Act.

(6) Openness Principle

With regard to a personal information file kept by the government agency, the agency shall publicize the name, classification, and scope of the file, the government agencies keeping or using the file, means of collecting personal information, etc, pursuant to Article 17 of the Personal Information Protection Act. However, non-government agency is not required to publicize the personal information file as the government agency is under the Personal Information Protection Act.

(7) Individual Participation Principle

An individual has the right to inquire, review, make copies of, correct or supplement her personal information file kept by information collectors and, in case of a dispute about the accuracy of personal information, to require information collectors to stop the use, processing or sharing of her personal information, pursuant to Articles 3, 10, and 11 of the Personal Information Protection Act.

Taipei, November, 2001).

(8) Accountability Principle

An information collector, a government agency or non-government agency, who infringes upon the rights and interests of an individual in violation of any provisions of the Personal Information Protection Act shall be liable for the damages arising therefrom. The total amount of compensation for the damages by an information collector shall be no less than NT$500 but no more than NT$20,000 for each case of damages per person in the cases where the victims may not or cannot provide evidence for actual damage amount, pursuant to Paragraph 3 of Article 28 and Paragraph 2 of Article 29 of the Personal Information Protection Act. However, according to Paragraph 2 of Article 28 and Paragraph 2 of Article 29 of the Personal Information Protection Act, the total maximum amount of compensation, which an information collector shall pay to the concerned individuals for damages caused by the same fact, increases to NT$200 million from the original NT$20 million.

In addition, an information collector who intends to make unlawful profits for himself or for a third party, or intends to infringe upon the interests of others by illegally changing or deleting personal information files, or by other illegal means and has impeded the accuracy of other people's personal information files and caused damages to others should be imposed of an imprisonment or custody of no more than 5 years, or a fine of no more than NT$1,000,000, or both, pursuant to Article 42 of the Personal Information Protection Act.

Before the passage of the current Personal Information Protection Act, which becomes effective on October 1, 2012, information collectors who infringed upon an individual's rights and interests in violation of any provisions of the Taiwanese Computer-Processed Personal Information Protection Act (CPPDPL), replaced by the current Personal Information Protection Act, should be also liable for the damages arising therefrom. The total amount of compensation for the damages should not be less than NT$20,000 but not more than NT$100,000 for each case of damages per person unless the injured individual could prove that the damages suffered by her were more than the aforesaid prescribed amount. With regard to damages caused to the individual by the same cause and fact, the total amount of compensation should not be more than NT$20 million. However, due to the cap on the total compensation amount, the compensation distributed to each individual would be likely less than NT$ 20 (about US$ 60 cents) as a result of a common but illegal sale of a database disc which easily contains more than one million individuals' personal information.[30] As a consequence, the injured individuals had no incentive to monitor and detect those information collectors who failed to live up to

their privacy promises, and to enforce privacy contracts.

To effectively protect information privacy, since October 1, 2012, the cap on the compensation amount has been removed or raised to strengthen the individuals' incentive to enforce their rights in personal information, and the mechanism of class action has been introduced to the current Personal Information Protection Act, in which case a consumer protection group has the right to bring litigation on behalf of a mass of consumers to enforce their rights. Furthermore, like punitive damages under the Taiwanese Consumer Protection Law,[31] punitive damages can be also introduced to the current Information Protection Act in the future, in which case the injured individual may claim for punitive damages up to three times of the amount of actual damages as a result of injuries caused by the willful act of misconduct of information collectors, provided, if such injuries are caused by negligence, a punitive damage up to one time of the amount of the actual damages may be claimed.

To cover the liability under the Information Protection Act or other applicable laws, the Bankers Association of the ROC (Taiwan) proposes to create a new insurance policy to cover all liability arising from customer personal information leakage accident in a maximum insurance amount of NT$ 20 million for the same cause and fact.[32] However, as insurance shifts risk from the insured to the insurer, the insured can externalize risk. Moreover, externalizing risk leads the insured to reduce precautions. The insurance industry calls the reduction in precaution affected by insurance as a moral hazard. Insurance firms make use of various methods of decreasing moral hazard, particularly co-insurance, deductibles, and experience rating.[33] Nevertheless, under the proposal of the Bankers Association of the ROC (Taiwan) that all liabilities will be covered by insurance, the insured will have "perfect insurance," such that "the insured is indifferent between having no accidents, or having an accident and making a claim."[34] In short, the insured will not care about accidents. Thus, the insured will have no incentive to employ and enforce security safeguard measures to prevent personal

30) See Yu-Ting Chen, Ge Zi Wai Xie Yin Hang XunQiuBao Hu (Banks Seek Protection as a Result of Personal Information Leakage), Chinatimes Daily, October 28, 2004.

31) According to Article 51 of the Taiwanese Consumer Protection Law, "In a litigation brought in accordance with this law, the injured consumer may claim for punitive damages up to three times of the amount of actual damages as a result of injuries caused by the willful act of misconduct of business operators, provided, if such injuries are caused by negligence, a punitive damage up to one time of the amount of the actual damages may be claimed."

32) See Yu-Ting Chen, Ge Zi Wai Xie Yin Hang Xun Qiu Bao Hu (Banks Seek Protection as a Result of Personal Information Leakage), Chinatimes Daily, October 28, 2004.

33) See Robert Cooter & Thomas Ulen, Law and Economics 354-355 (4th ed. 2004).

34) See id. at 355.

information from unauthorized access or use, or leakage. In this connection, to protect consumer personal information, the proposed perfect insurance policy should be prohibited or replaced by a co-insurance or deductibles policy.

(9) Limitations on International Transfer of Personal Information

The international transfer of personal information conducted by government agencies shall be in compliance with relevant laws and regulations. As for international transfer of personal information conducted by private industries, competent authorities, such as the Ministry of Justice, may limit such international transfer, 1) when a data-receiving country fails to provide an adequate level of information privacy protection and, thus, is likely to cause damages to a data subject; or 2) when personal information is transferred to a third country by a circuitous means to circumvent the applicable laws, pursuant to Article 21 of the Personal Information Protection Act.

Like the EU Data Protection Directive, the Personal Information Protection Act prohibits the cross-border transfer of personal information from Taiwan to any third countries lacking an adequate level of information privacy protection. However, as the advance of computer and Internet technology makes it extraordinarily difficult and expensive for governments or individuals to detect and control the dissemination of personal information, such information is in fact illegally widespread inside and outside of Taiwan.

5. The Costs of Protecting Personal Information

Information privacy focuses on protecting an individual's right to define his or her self.[35] An inward and outward focus of personhood is essential to the establishment of an individual's identity. However, although information privacy is necessary to one's quality of life in modern world, it is obvious that some real costs are imposed by the granting of privacy. Opportunities to be misleading are inherent in legal protection for "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[36] Therefore, information privacy could facilitate the distribution of incorrect information by making the

35) See Richard C. Turkington, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. Ill. U. L. Rev. 479 (1990).

36) See Alan F. Westin, Privacy and Freedom 7 (1967).

discovery of falsehoods difficult or even impossible. For example, a job applicant might lie about his employment records. Similarly, information privacy could block the sharing of relevant true information. For instance, consumers' safety might be endangered due to the failure of an airline pilot to disclose a medical condition that could affect his job performance. Information privacy limits the collection, use, processing or sharing of personal information that government, businesses, and others could draw upon to make rapid and informed decisions, such as whether to provide social aid or accept a check. As a result, the costs of information privacy are high. These include both transactional costs to information users of ascertaining the accuracy and completeness of the information they collect, and the risk of future losses caused by incomplete and inaccurate information. In other words, information privacy might reduce productivity and make services and products more expensive.[37)]

Therefore, it is evident that neither information privacy costs nor values are absolute. One person's information privacy interests may contradict another's or society's, and may ever contradict some of his own, other interests. It is necessary to balance the different interests.[38)] In cases of failure to take into account the variety and importance of contextual factors and competing values, such as public interests, commerce, and truthfulness, it will be not workable to protect information privacy.

Ⅲ. The Developments and Regulations of National Identification Card Numbers in Taiwan

Information privacy limits the collection, use, processing or sharing of personal information that necessary for government, businesses and others to make rapid and informed decisions. However, declining to provide information collectors with personal information to verify one's identify is not a reasonable option, unless he or she is willing to forgo a large and ever-increasing portion of everyday products, services or activities. Thus, in modern society people frequently disclose personal information for various specific purposes and then information collectors might provide them with credit card numbers, bank account numbers, phone numbers, driver's license numbers, club membership numbers, student ID numbers, and so on for identification authentication and linking to

37) See Fred H. Cate, Privacy in the Information Age 28-29 (1997).
38) See id.

databases. Similarly, national Identification cards and their numbers might be assigned by government for identifying individuals.

More than 100 countries, including Taiwan, have some form of national Identification card and numbering system. A national Identification system consists of linking a database of information about individuals to an identifier, such as a national Identification card number, so that individuals will be readily connected to a stream of data about them. Proponents of a national Identification system point to advance efficiencies, ease of access, prevention of fraud, and capacity to screen for criminals and terrorists. However, critics content that a national Identification system can increase the risks[39] to invade the privacy if the national Identification card or its number is lost, stolen or abused. The following are the developments and relevant regulations of National Identification Card Numbers in Taiwan.

1. The Generation and Assignment of National Identification Card Numbers

A National Identification Card of the ROC (Taiwan) is used to identify a person, and is effective throughout the country.[40] Each citizen is qualified to apply for one National Identification Card. Each citizen who has reached the age of 14 is bound to apply for a National Identification Card for the first time.[41] In addition, who is under 14 years old may also apply for a National Identification Card.[42] ID photos should be submitted to apply for a National Identification Card.[43] If a person has lost or damaged his/her National Identification Card, he or she shall apply for re-issuing.[44] When a person applies for household registration and that results in changes on National Identification Card information, he or she shall at the same time apply for a replacement of his/her National Identification Card.[45] Each citizen must always carry his or her National Identification Card. A National Identification Card shall not be detained unless in accordance with the law.[46]

Each citizen shall be assigned a National Identification Card Number upon birth and household,

39) See Daniel J. Solove and Marc Rotenberg, Information Privacy Law 454-455 (2003).
40) Household Registration Act (戶籍法), art. 51.
41) Household Registration Act (戶籍法), art. 57.
42) Household Registration Act (戶籍法), art.57.
43) Regulations Governing the Establishment of Photo Files for National Identification Card and Household Certificate(art.10.
44) Registration Act (art. 57.
45) Registration Act (art. 58.
46) Registration Act (戶籍法), art. 56.

including naturalization, registration by a household registration office.[47] Each citizen under 12 years of age shall be subject to birth registration.[48] The application for birth registration shall be filed by the parents, grandparents, head of the household, cohabitant or foster parents of the newborn within 60 days after birth.[49]

The National Identification Card Number shall be assigned by sequence and, in case of repetition or mistake, may be corrected or replaced by the household registration office.[50] In the past, the personal information contained in the National Identification Card was filled out by handwriting; therefore, it was more likely to have repetition in the National Identification Card Number, leading to embarrass the other person with the same number. However, nowadays the repetition of numbers only happens in unusual cases as a result of the usage of computer system to interconnect different household registration offices. As each citizen will be assigned a unique National Identification Card Number, each generally owns a different number from others. A National Identification Card Number consists of ten codes, one English alphabet and nine Arabic numerals (digits), in which case the first code is one English alphabet, standing for specific one of 22 cities and counties in Taiwan where to apply with government for birth registration, and the second to tenth codes are Arabic numerals that the second one stands for gender and the tenth for check code.[51]As for the code of birth registration place, for example, English alphabet “A” is for Taipei City, the capital of Taiwan, alphabet “B” is for Taichung City, located in central Taiwan, and “E” is for Kaohsiung City, located in southern-western Taiwan. As for gender code, Arabic numeral “1” is for male, and “2” for female. In contrast to Korean system, the National Identification Card Number system adopted in Taiwan does not directly refer to or reveal any personal information of a National Identification Card holder, like date of birth. However, it still implicates the personal information of a National Identification Card holder, like gender and the original place of birth registration.

47) Regulations Governing the Establishment of Photo Files for National Identification Card and Household Certificate (國民身分證及戶口名簿製發相片影像檔建置管理辦法), para1 of art. 6.
48) Household Registration Act (戶籍法), art. 6.
49) Household Registration Act (戶籍法), arts. 29 and 48.
50) Regulations Governing the Establishment of Photo Files for National Identification Card and Household Certificate(國民身分證及戶口名簿製發相片影像檔建置管理辦法), art. 7.
51) Regulations Governing the Establishment of Photo Files for National Identification Card and Household Certificate(國民身分證及戶口名簿製發相片影像檔建置管理辦法), art. 5.

(front side of ID Card specimen)

(back side of ID Card specimen)

2. The Brief History of National Identification Card Numbers

Before 1965, Taiwan had issued National Identification Cards to her citizens, but National Identification Card Number system was not adopted yet. In 1965 the government adopted a new reform to National Identification Card and begun to assign a serial number to its holder. On April 17, 1965 Yaming Mountain Administration Bureau in Taipei area issued the first one of newly-revised version of National Identification Card to President Chiang Kai-shek, including his National Identification Card Number— Y10000001. At that time, the National Identification Card Number only had nine codes and lacked one check code. After 1969, the check code was added to National Identification Card Number system due to computer processing, and each citizen was immediately assigned a National Identification Card Number upon birth registration.[52)]

3. The Unconstitutionality of "New Identification Card not to Issue without Fingerprint"

With respect to the relevant provisions of Article 8-II and III of the Household Registration Act, stating to the effect that the new ROC Identification (identity) card will not be issued without the applicant being fingerprinted, the Council of Grand Justices in 2005 in its "Interpretation of Council of Grand Justice No.603" held them unconstitutional. Grand Justices find, fingerprints are important information of a person, who shall have self-control of such fingerprinting information, which is protected under the right of information privacy. However, the issuance of ROC identity cards will directly affect the people's exercise of their fundamental rights. Article 8-II of the Household

52) The development of the ROC National Identification Card, https://zh.wikipedia.org/wiki/%E4%B8%AD%E8%8F%AF%E6%B0%91%E5%9C%8B%E5%9C%8B%E6%B0%91%E8%BA%AB%E5%88%86%E8%AD%89.

Registration Act provides, “While applying for an ROC identity card pursuant to the preceding paragraph, the applicant shall be fingerprinted for record keeping; provided that no national who is under fourteen years of age will be fingerprinted until he or she reaches fourteen years of age, at which time he or she shall then be fingerprinted for record keeping.” Article 8-III thereof provides, “No ROC identity card will be issued unless the applicant is fingerprinted pursuant to the preceding paragraph.” Refusal to issue an ROC identity card to one who fails to be fingerprinted according to the aforesaid provisions is no different from conditioning the issuance of an identity card upon compulsory fingerprinting for the purpose of record keeping. The failure of the Household Registration Act to specify the purpose thereof is already inconsistent with the constitutional intent to protect the people’s right of information privacy. Even if it may achieve such objectives as anti-counterfeit or prevention of false claim or use of an identity card, or identification of a roadside unconscious patient, stray imbecile or unidentified corpse, it fails to achieve balance of losses and gains and uses excessively unnecessary means, which is not in line with the principle of proportionality. The relevant provisions of Article 8-II and III of the Household Registration Act, providing to the effect that no ROC identity card will be issued unless an applicant is fingerprinted for record keeping, are inconsistent with the intent of Articles 22 and 23 of the Constitution, and thus shall no longer apply as of the date of this Interpretation.

4. The Use of National Identification Card Numbers

As mentioned above, each citizen will be assigned a National Identification Card Number upon birth registration by a household registration office.[53] Because no two persons normally possess the same number, the potential confusion that might occur if to use names and dates of birth can be avoided. Unlike names and addresses, National Identification Card Numbers generally do not change and thus provide consistency over time. The use of National Identification Card Numbers by entities other than the household registration offices is not inherently objectionable, so National Identification Card Numbers are in many ways ideally suited as unique identifiers. Further, the existence and use of a common identifier is virtually indispensable in allowing public or private organizations to differentiate

53) Regulations Governing the Establishment of Photo Files for National Identification Card and Household Certificate(國民身分證及戶口名簿製發相片影像檔建置管理辦法), para. 1 of of art. 6.

one individual from another. For example, libraries should have a means for identifying those who are borrowing books; banks should have a means to match deposits to accounts; and schools should have a means to track academic records. A unique identifier allows these types of transactions and processes to occur efficiently. Not surprisingly, the National Identification Card Numbers have been credited with facilitating coordination among government agencies and private corporations.[54)]

As the National Identification Card Number, together with other basic personal information including but not limited to name, date of birth, place of birth, and address, is not only printed and shown on the National Identification Card, but also on the National Health Insurance Identification Card, and the driving license, one or two of these three certificates are normally required to show and used to verify or authenticate one's identity for the purposes of initiating, processing or completing contacts, applications or transactions with government or industries in Taiwan. Therefore, *through "identification authentication[55)]", information collectors, government or industries, will collect, process, use, or share personal information, including their National Identification Card Numbers, for the purposes of education, opening banking account, insurance, telecommunication service, land ownership registration, taxation, military service, marriage registration, street demonstration application, corporation formation application, donation of reproductive cells, criminal records, death notification, etc.*

As Ira Bloom noted, "[a] person cannot function normally in today's United States without a social security number."[56)] Nowadays in Taiwan, an individual's National Identification Card Number is also frequently obtained as a matter of course to uniquely identify both the individual and his or her account, either in the traditional or e-commerce digital environment. When one person is applying for approval with government agency, or is seeking medical care or renting an apartment, the agency or service-providing entity will frequently obtain a National Identification Card Number as a prerequisite to complete application or business. The entities unrelated to the household registration offices are also

54) See Jonathan J. Darrow & Stephen D. Lichtenstein, "DO YOU REALLY NEED MY SOCIAL SECURITY NUMBER?" DATA COLLECTION PRACTICES IN THE DIGITAL AGE, 10 N.C. J. L. & Tech. 1, 4-5 (Fall 2008).

55) "Identification authentication is the process whereby evidence of identity is assessed in order to establish a sufficient degree of confidence that data is being associated with the correct human being." See Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues, https://digitalcollections.anu.edu.au/bitstream/1885/46248/27/03Paper02.pdf.

56) See Ira Bloom, of Information Laws in the Digital Age: The Death Knell of Information Privacy, 12 Rich. J.L. & Tech. 9, 46 (2006).

allowed to request, collect, process, use or share customers' National Identification Card Numbers according to applicable laws in Taiwan. Therefore, the widely-use approach to the National Identification Card Numbers has also evolved into "a data collection practice that spans the gamut of organizations, from government agencies to non-profits, employers to financial services institutions, universities to health service providers, as well as credit card companies, retailers, and many others." The disclosure of a National Identification Card Number is a critical necessity to engage in a wide range of daily activities in modern society. If a person is an active participant in the modern economy, the list of companies that have his or her National Identification Card Number is depressingly long.[57)]

As Jonathan J. Darrow and Stephen D. Lichtenstein noted, "the increasing reliance upon and importance of personally identifiable information in essence creates and defines a virtual person, described by one commentator as a digital persona that approximates personality. The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual."[58)] Therefore, like in the U.S., in today's Taiwan a person cannot function normally without a National Identification Card Number. However, it is also impossible for a person to function if his or her personally identifiable information, including National Identification Card Number, is widely disseminated to others, creating the opportunity for invasion of privacy and, especially, identity theft, which is also perhaps the fastest growing crime in Taiwan. Law enforcement, business and commerce already have recognized the value of personal information in many contexts, so government and industries go to great lengths to collect such information[59)] to establish databank, databases or dossiers.

As a result, the National Identification Card Number has become a unique personal identifier linked to various sources of information and public and private databases with respect to one specific person's family history, education, property, residence histories, and public transactions, etc.

57) See Jonathan J. Darrow & Stephen D. Lichtenstein, "DO YOU REALLY NEED MY SOCIAL SECURITY NUMBER?" DATA COLLECTION PRACTICES IN THE DIGITAL AGE, 10 N.C. J. L. & Tech. 1, 66 (Fall 2008).

58) See id. at 1-2.

59) See id.

5. The Database of Household Registration

As mentioned above, each citizen shall be subject to birth registration and, then, will be assigned a unique National Identification Card Number upon birth registration by a household registration office. That National Identification Card Number will be tied to the specific household registration records of that number holder kept by the household registration offices. According to Article 4 of the Household Registration Act, the household registration above in Taiwan includes the following registrations: 1.registrations of personal status, including: (1) birth registration, (2) registration of parentage, (3) adoption and adoption termination registration, (4) marriage and divorce registration, (5) registration of legal guardianship, (6) assistance registration, (7) registration of exercising responsibility of the rights and obligations for minor children, (8) registration of death and presumption of death, (9) registration of indigenous status and tribe group; 2. initial household registrations; 3. registrations of movement, including: (1) moving-out registration, (2) moving-in registration, (3) address alteration registration; 4. household separation (combination) registration; 5. birth place registration; and 6. other registrations according to other applicable laws.[60] As the household registration records of a data subject are still kept even after death, a National Identification Card Number can track not only the household registration records of a specific living person, but also those of his or her spouse, parents, descendants, and ancestors back to the period of Japanese colony beginning to establish the household registration system in 1906[61]. Through internet a household registration office may interconnect and access the household registration records collected by other household registration offices. The household registration has slowly evolved into a massive databank or database containing cradle-to-grave records for every Taiwanese citizen. The databank would contain every person's and his or her relatives' records of birth certificate, gender, proof of citizenship, address, education level, military service, marriage, race, and ultimately, death.

As a matter of fact, in addition to household registration offices having right to collect, process, and use the household registration records for household purpose, other government agencies or private entities may access such records for other applicable purposes pursuant to Articles of 16 and 20 of the Personal Information Act. Therefore, government agencies other than household registration offices

60) Household Registration Act (戶籍法), art. 4.

61) http://e-household.hccg.gov.tw/web/SelfPageSetup?command=display&pageID=20788&FP=D30000001923000001_16.

may also easily have administrative access to the centralized household registration database for the purpose of law enforcement. For example, the police, prosecutors, courts may collect, process, and use the specific household registration records of a suspect or defendant for crime investigation.

6. The Sharing of Databases by Using National Identification Card Numbers

Personal information shall be used in compliance with the specific purpose of original collection unless otherwise provided by laws or agreed by the concerned individual, pursuant to Articles 16[62] and 20[63] of the Personal Information Protection Act.

As a result, according to Section 1 of Paragraph 1 of Article 16 of the Personal Information Protection Act, the police, prosecutors, judges or other government officials are allowed to share and obtain the personal information of a specific person from databases collected and maintained by other government agencies or private entities for purposes, such as crime investigation, trial process, application for social aid, as authorized by other laws and regulations, such as Article 247 of the Criminal Procedure Law[64], Article 65-1 of the Household Registration Act[65], Article 44-3 of the

62) According to Article 16 of Personal Information Protection Act, "the government agency should use the personal information in accordance with the scope of its job functions provided by laws and regulations, and in compliance with the specific purpose of collection. However, the information may be used outside the scope upon the occurrence of one of the following conditions: 1.it is in accordance with law; 2.it is necessary for national security or promotion of public interests; 3.it is to prevent harm on the life, body, freedom or property of the Party; 4.it is to prevent harm on the rights and interests of other people; 5.it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after its processing by the provider, or from the disclosure by the collector; 6.such use may benefit the Party; and 7.consent has been given by the Party."

63) According to Article 20 of Personal Information Protection Act, "Except the information stated in Paragraph 1 of Article 6, the non-government agency should use the personal information in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside the scope upon the occurrence of one of the following conditions: 1.it is in accordance with law; 2.it is necessary to promote public interests; 3.it is to prevent harm on the life, body, freedom or property of the Party; 4.it is to prevent harm on the rights and interests of other people; 5.it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after its processing by the provider, or from the disclosure by the collector; 6.consent has been given by the Party; 7.such use benefits the Party."

64) "A public prosecutor may request from a competent public office any report necessary to an investigation."

65) "The applicants shall apply for their Kinsfolk Relation Record at any household registration office if they meet one of the following conditions: 1. Are required to verify family relationships as stipulated according to Article 15 or Article 29, the Artificial Reproduction Act. 2. Are required to verify family relationship for organ donation as stipulated according to Article 8, the Human Organ Transplant Regulation. 3. Are required to verify the descendent's spouse and the genetic relationship for Inheritance Registration. 4. Are required to verify their fathers or mothers are ROC nationals according

Public Assistance Act[66]. As a consequence, the police, prosecutors, judges or government officials heavily rely on the use of a National Identification Card Number to access, locate, and obtain the personal information of a specific person collected and maintained in a database for the purpose of law enforcement. For example, via directly interconnected computer system, the police, prosecutors, judges are allowed to, on a case-by-case base, directly access, locate, and obtain the personal information of a suspect or defendant from the nationwide centralized database of the household registration, collected and maintained by the central and local household registration offices, by entering his or her National Identification Card Number. *For another example, as for the application for social aid, when a social worker hired by a government agency files an application for social aid by entering the National Identification Card Number of the applicant, then the government will automatically send a electronic file, containing the basic information of the close relatives of the applicant, and their taxation and property information, to the social worker to review the qualification and necessity of the applicant for applying social aid.*

As for private industries, when a person intends to open a banking account, he or she has to provide the bank with his or her personal information, including name, birthday, National Identification Card Number, address, telephone number, so as to verify or authenticate his or her identity for the purpose of entering into and completing the agreement. Thus, during the term of the agreement, the bank will collect customers' personal information which can be categorized as follows: (1) basic information, including individual's name, date of birth, National Identification Card Number, telephone number, address, etc., (2) account balance information, including account number, credit card number, deposit, loan, and other transaction or financial information, (3) credit information, including record of check bounced, record of debt written off, business situation, etc., and (4) investment information, including investment object, amount, date, etc..[67]

According to Sections 1 and 6 of Paragraph 1 of Article 16 of the Personal Information Protection

---

to Article 2, Nationality Act. 5. Are required by court or trial to verify their Kinsfolk Relation Record.
6. Are required to verify their Kinsfolk Relation Record according to other laws."

66) "The competent authority may ask the relevant authority (institutions), Associations, corporations or individuals to provide the necessary information needed for the operation of the support efforts under this Act. The competent authority shall properly practice the fiduciary duty for the information gained through the above description. The competent authority shall conduct a safety check on the operation of information; with the retention, processing and utilization of the information being subject to the Personal Information Protection Act."

67) Regulations for Managing the Cross-selling among Subsidiaries of a Financial Holding Company (金融控股公司子公司間共同行銷管理辦法), para. 2 of art. 10.

Act, the non-government agency should use the personal information in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside the scope upon the occurrence of one of the following conditions: "1.it is in accordance with law; ……; 6.consent has been given by the Party." Thus, the bank should not share a customer's personal information with any third party unless otherwise provided by law or consented by the customer.

Therefore, according to Paragraph 1 of Article 26 of the Regulations Governing Authorization and Administration of Service Enterprises Engaged in Interbank Credit Information Processing and Exchange, financial institutions should submit pertinent information about loans, credit cards and financial derivatives business to the service enterprise engaged in interbank credit information processing and exchange. Currently, the service enterprise engaged in interbank credit information processing and exchange is the Joint Credit Information Center (JCIC). In 1975 the JCIC was established under the Bankers Association of Taipei and responsible for collecting, processing, and exchanging credit data among financial institutions. The JCIC is the only domestic credit-reporting agency in Taiwan. It not only collects positive and negative personal and business credit information, but also develops a personal and credit-scoring system, so as to enable financial institutions to access credit by this credit information database.[68] In addition, when a person wishes to borrow money from a bank, he or she has to authorize the bank to use his or her personal information, including National Identification Card Number, to obtain his or her credit report from the JCIC.

8. The Security Safeguards and Misuse of Databases

The information collectors shall have specific security safeguard plans to prevent personal information collected from being stolen, altered without authorization, damaged, lost or disclosed, pursuant to Articles 6, 18 and 27 of the Personal Information Protection Act.

Furthermore, the information collectors, the government agency or the non-government agency, shall take proper technical or organizational measures for the purpose of preventing personal information from being stolen, altered, damaged, destroyed or disclosed. The measures above-mentioned may include the following matters and shall follow the principle of appropriate proportionality to achieve the objective of personal information protection: (1) allocating management

68) http://www.jcic.org.tw/main_en/index.aspx

personnel and substantial resources; (2) defining the scope of personal information; (3) establishing the mechanism of risk evaluation and management of personal information; (4) establishing the mechanism of preventing, giving notice of, and responding to accidents; (5) establishing an internal management procedure of collecting, processing, and using personal information; (6) managing information security and personnel; (7) promoting acknowledgement, education and training; (8) managing facility security; (9) establishing a mechanism of auditing information security; (10) keeping records of the use, locus information and proof; and (11) Integrated persistent improvements on the security and maintenance of personal information, pursuant to Article 12 of the Enforcement Rules of the Personal Information Protection Act.

As mentioned above, the information collectors, such as the police, prosecutors, judges, other government officials, household registration offices, financial institutions, and the Joint Credit Information Center, shall take proper technical or organizational measures for the purpose of preventing personal information, such as National Identification Card Number, from being stolen, altered, damaged, destroyed or disclosed. However, there are occasional cases[69] of misusing or leaking personal information of citizens or customers. For example, in the past decade there were several cases involving policemen for bribes respectively leaking to the debt collectors or gangsters the latest registered addresses of absence debtors by using their National Identification Card Numbers to access the interconnected database of the household registration. For another example, a widowed judge searched for personal information of his blind dates or unmarried female colleagues through the interconnected database of the household registration. However, as the staff of the court which the judge worked tracked down the records of his illegitimate use, he was impeached and finally left office.

In recent years, law enforcement officers have increasingly used advanced technologies, facilities and data-mining methods to collect data in public spaces and even to compare data from public and private various databases, such as the nationwide centralized database of the household registration. The establishment and use of the facial-recognition system in the M-police (Mobile-Police) Operation System is one example. The police are provided with the M-Police mobile device, a powerful tool utilizing the latest technologies to collect evidence on the crime scene and to assist those people with dementia to return home. The device is equipped with an assortment of value-added applications,

69)http://city.udn.com/54532/4846770#ixzz49luGNoAA

including search function for personal information.[70] With the M-police device, the police can immediately search for and obtain the personal information of a specific pedestrian, such as name, birthday, National Identification Card Number, address, by taking a photo of his/her face and then comparing with the nationwide ID photos files contained in the centralized database of the household registration. As the capability of the M-Police mobile device to recognize the identities of any data subjects is quite powerful, many congressmen and privacy advocates who worry its misuse and invasion of privacy strongly oppose its establishment and use. As a result, the M-police plan is finally aborted.

Actually, the facial-recognition function of the M-police equipment will seriously invade the desire of individuals for times of "public privacy," which is the core of the anonymity. As Alan Westin mentioned, one state of privacy is anonymity, occurring when "the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known those observing him. In this state the individual is able to merge into situational landscape. Knowledge of fear that one is under systemic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas…."

9. Profiling by Using National Identification Card Numbers to Link to Various Databases

As mentioned above, the National Identification Card Number is a unique personal identifier linked to various sources of information and public and private databases (databanks) with respect to one specific person's date of birth, address, family history, education, property, residence histories, financial records, business transactions, employment, social security, taxation, and medical treatment, etc. As such, the National Identification Card Number has become a critical tool for government agencies and private industries to interconnect with multiple sources and collect personal information. By using the National Identification Card Number, the government agencies and private industries can

70) https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=72977&ctNode=12835

effectively collect personal information from various databases. **These data would paint a detailed portrait of each individual's habits and preference even though such collections would not be fully accurate, secure or updated.**[71]

By using the National Identification Card Number and other personal information to collect, combine and aggregate information from multiple sources collecting disparate pieces of information, the government agencies and private industries can create information mosaics. "This would infuse information that, standing alone, might have been inconclusive without meaning gleaned from other sources. These collections of details on individuals' lives contribute to serious invasions of privacy, ongoing surveillance of lawful activities, and chilling effects on political involvement and expressions."[72]

As Daniel J. Solove noted, any national system of identification, such as the database of Taiwanese household registration, would ultimately be offensive and intrusive to fundamental rights. Although people may be aware that dossiers or databases are being assembled about them, they have no exact idea what information the dossiers contain or how the dossiers are being used. The problem with information collection and use today is not merely that individuals are no longer able to exercise control over their information; it is that their information is subjected to a bureaucratic process that is itself out of control. Without this process being subject to regulation and control and without individuals having rights to exercise some dominion over their information, individuals will be routinely subjected to the ills of bureaucracy.[73]

In Taiwan, Section 1 of Article 8 and Section 1 of Article 9 of the Personal Information Protection Act explicitly obligate the government agencies and private industries to provide adequate knowledge to individuals about the purposes for what and how personal information is to be collected, used or shared. Therefore, the government agencies and private industries shall explain to the concerned individual the purposes of collection, use or sharing of personal information in order to obtain the required consent, by providing a clear and sufficient notice to the individual. However, according to Section 2 of Article 9 of the Personal Information Protection Act, the government agencies and private

71) See Richard Sobel, THE DEGRADATION OF POLITICAL IDENTITY UNDER A NATIONAL IDENTIFICATION SYSTEM, 8 B.U. J. Sci. & Tech. L. 37, 46 (Winter 2002).

72) See id. at 70.

73) See Daniel J. Solove, ACCESS AND AGGREGATION: PUBLIC RECORDS, PRIVACY AND THE CONSTITUTION, 86 Minn. L. Rev. 1137, 1194 (June, 2002).

industries do not have to provide adequate knowledge to individuals about the purposes for what and how personal information is to be collected, used or shared if the government agencies perform their official duties or private industries fulfill their legal obligation. As a result, when the sharing of personal information contained in various databases, such as the household registration database or the credit information database, among the information collectors, such as the police, prosecutors, judges, other government officials or financial institutions, is to perform their official duties or fulfill their legal obligation, the individuals will not be informed of the sharing of their personal information. In such a case, the individuals will live in a world "where dossiers about individuals circulate in an elaborate underworld of public and private sector bureaucracies without the individual having notice, knowledge, or the ability to monitor or control the ways the information is used?[74]" In particular, the collection, processing and use of personal information are used to make decisions affecting an individual's life; however, individuals often have no way to participate and no notice about what is happening.

Furthermore, similar to Richard Sobel's comment, the Taiwanese household registration and other databases provide the government and even private industries with a back door to get personal information. Due to the ease of access, centralized or interconnected databases make Identification Card and its number checks simple and routine. If there is no probable cause to check databases or demand identification, it will facilitate further routine intrusions that destroy the privacy protections in personal spaces against unnecessary scrutiny. In particular, the requirements for Identification Card and its number in order to work, travel or conduct transactions, and the ease to access various databases, will destroy the most basic freedoms − the right to be left alone in privacy and anonymity unless there are compelling reasons for intrusions.[75]

In fact, as Richard Sobel noted, "the history of discriminatory and oppressive uses of identity badges, identity numbers, and databanks against Jews in Germany, Blacks during slavery in the U.S. and under Apartheid in South Africa, and Japanese-Americans during World War II in the U.S. should create wariness of the problems caused by quick fixes like identity documents."[76] Consequently, if the Taiwanese household registration or other databases cannot be adequately safeguarded against privacy

74) See id. at 1195.

75) See Richard Sobel, THE DEGRADATION OF POLITICAL IDENTITY UNDER A NATIONAL IDENTIFICATION SYSTEM, 8 B.U. J. Sci. & Tech. L. 37, 68 (Winter 2002).

76) See id. at 71.

invasions and abuses, any national system of identification, such as National Identification Card Number, would ultimately be a peril to fundamental rights rather than a useful social tool.

Ⅳ. Conclusion

Before 1965, Taiwan had issued National Identification Cards to her citizens, but National Identification Card Number system was not adopted yet. In 1965 the government adopted a new reform to National Identification Card and begun to assign a serial number to its holder. Each citizen is qualified to apply for one National Identification Card and will be assigned a National Identification Card Number upon birth and household registration by a household registration office.

Because no two persons normally possess the same number, the potential confusion that might occur if to use names and dates of birth can be avoided. Unlike names and addresses, National Identification Card Numbers generally do not change and thus provide consistency over time. Further, the existence and use of a common identifier is virtually indispensable in allowing public or private organizations to differentiate one individual from another. A unique identifier allows these types of transactions and processes to occur efficiently. Not surprisingly, the National Identification Card Numbers have been credited with facilitating coordination among government agencies and private corporations. Therefore, through identification authentication, the information collectors, such as government and industries, will collect, process, use, or share massive personal information, including their National Identification Card Numbers, for various purposes.

By using the National Identification Card Number and other personal information to collect, combine, aggregate, and share information from multiple sources or databases, the government agencies and private industries can create information mosaics. However, if there is no probable cause to check databases or demand identification, it will facilitate further routine intrusions that destroy the privacy protections in personal spaces against unnecessary scrutiny.

In addition, the information collectors shall take necessary security safeguard measures to prevent personal information collected from being stolen, altered without authorization, damaged, lost or disclosed. If the databases cannot be adequately safeguarded against privacy invasions and abuses, any national system of identification, including National Identification Card Number, would ultimately be

a peril to fundamental rights rather than a useful social tool.

In particular, when personal information, including National Identification Card Number, is unprotected and distributed easily and widely, the information will form the individual's social identity, and thus affect the identity that the individual actually establishes.[77] Thus, it is reasonable to grant individuals a right to control the dissemination of personal information about them. Furthermore, due to the wide proliferation of information technologies, the skyrocketing of the volume of personal information created and collected, and the decline of the cost of processing personal information, the perceived need to protect information privacy is increasing.

77) See Julia C. Schiller, Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?,11 CommLaw Conspectus 351 (2003).

대만의 주민등록번호 체제의 법적 쟁점

Ⅰ. 서론

일상생활에서 방대한 양의 개인 정보가 수집·처리·사용·공유되어지면서, 사이버 시대에서 개인의 사생활정보는 큰 위험에 처해있다.[1] 유진 볼로흐(Eugene Volokh)는 자기정보통제권을 "자신을 나타내는 개인 정보를 사용하는 상대방을 통제 할 수 있는 나의 권리"라고 정의하고 있다.[2]

자기정보통제권은 개인의 사생활권리의 하위 범주이다.[3] 사실상, 제리 강(Jerry Kang)에 따르면, "사생활"이란 용어는 많은 개념이 포함되어 있는데, 이는 세 가지로 분류되어질 수 있다. 첫 번째 개념은 개인의 공간을 타인으로부터 침해당하지 않도록 보호해야하는 "물리적 공간"을 말한다. 이 사생활 공간은 개인의 공간 대 공공의 공간이라는 논쟁을 포함한다. 두 번째 분류체계는 국가의 간섭 없이 개인 의사 결정을 할 수 있는 자유를 말한다. 이 "결정할 자유의 사생활"는 논쟁이 되었던 대부분의 정치와 헌법 문제를 일으켜왔다.[4] 세 번째 하위그룹은 개인정보의 전파를 의미한다. 이 "사생활정보"는 개인정보의 수집·처리·사용·공유에 대한 대인의 통제권에 관한 것이다.[5]

미국의 사회 보장 번호(Social Security number, SSN)와 대만의 주민등록번호(Identification Card Number)는 개인의 신분을 식별할 수 있는 개인정보 중의 하나이다. 대만에서, 개개인은 주민등록번호(National Identification Card Number)는 호적사무소에서 출생이나 귀화등록에 의거해 배정되어진다. 두 사람이 같은 번호를 사용할 수 없으므로, 주민등록 번호가 아닌 이름과 출생일을 사용하는 경우에 생기는 잠재적 문제를 막을 수 있다. 각개인은 숫자라는

---

1) 참고 Susan E. Gindin, Lost and Found in Cyberspace: Information Privacy in the Age of the Internet, 34 San Diego L. Rev. 1153 (1997)

2) 참고 Eugene Volkh, Cyberspace and Privacy: A New Legal Paradigm? Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1073-74 (May 2000)

3) 참고 Eugene Volkh, Cyberspace and Privacy: A New Legal Paradigm? Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1073-74 (May 2000)

4) 참고 Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1202-1203 (1998).
"결정할 자유의 사생활"은 Roe v. Wade, 410 U.S. 113 (1973)에서 주로 논의되어졌다. Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) 논문은 사생활의 권리를 아이를 가질 수 있는 결정권까지를 포함한고 주장한다. Griswold v. Connecticut 381 U.S. 479, 485-86 (1965)논문은 피임약의 사용을 금지법이 부부사이의 사생활 권리는 헌법에 명시된 권리를 침해한다고 주장한다.

5) 참고 id.

독특한 방법으로 식별된다. 이는 곧 정부가 발행한 숫자를 통해서 개인에 대한 자료 수집이 요람에서 무덤까지 추적되어지는 걸 의미한다. 공통적 식별 매체의 존재와 사용은 공, 사조직이 각 개인을 다른 사람으로부터 구분하기 위해 사실상 필수적이다. 그 결과, 국가 주민등록 번호와 그 외의 개인 정보의 수집 관행이 정부조직부터, 비영리단체, 금융서비스 기관, 학교, 병원, 신용카드회사, 소매상, 웹사이트까지 전반에 걸쳐 시행되고 있다. 그리고 그들은 이러한 정보를 토대로 데이터뱅크나 데이터베이스를 만든다.

현 시대에 각 개인이 주민등록번호 없이 삶을 영위하기란 어렵지만, 반대로 개인의 주민등록번호를 포함한 개인 신분정보가 사생활 침해의 여지를 남기며 다른 사람에게 널리 퍼지게 되는 경우도 마찬가지로 삶을 영위하기가 어렵다. 특히 주민등록번호를 사용하여, 정부 기관과 개인 산업체는 다양한 데이터베이스로부터 효과적으로 개인정보를 수집하고, 결합한다. 개인의 취미와 선호에 대해 정확하거나 세부적이고 최신의 정보는 아닐지라도, 이렇게 수집된 자료들은 각 개인에 대해 꽤나 세부적인 정보를 제공한다. 이러한 점에서, 주민등록번호는 힘을 집중화하고, 동시에 우리는 정보가 힘의 원천인 시대에 살기 때문에 모여진 정보는 권력의 중심이 된다.[6)]

결과적으로, 정보 경제의 도래와 번영이[7)] 개인 정보에 대한 수요를 증가시키고 그 정보의 파급력 또한 방대하게 증가된다. 특히, 사이버 공간에서는 사생활정보가 희소한 자원이 되었다. 따라서 주민등록번호를 포함한 다른 정보에 대한 사생활정보와 개인정보의 수요 사이에서 균형을 찾는 점이 굉장히 중요한 문제가 되었다.

Ⅱ. 대만의 개인 정보 보호를 위한 법과 규제의 발전

1. 정보 사생활

미국 헌법에서와 같이, “사생활”이란 용어는 대만 헌법(the Constitution of the ROC)에 명확히 명시되어있지 않다. 헌법 제12조에 따르면, “대중은 통신기밀 자유를 가진다.” 그러므로 누군가의 편지를 공개하는 것은 개인의 사생활 침해로 해석 되야 한다. 게다가, 헌법 제 10

6) 참고 Richard Sobel, THE DEGRADATION OF POLITICAL IDENTITY UNDER A NATIONAL IDENTIFICATION SYSTEM, 8 B.U. J. Sci. & Tech. L. 37, 65 (Winter 2002)

7) 참고 Fred H. Cate, Data Protection Law and the European Union’s Directive: The Challenge for the United States: The EU Data Protection Directive, Information Privacy, and the Public Interest, 80 Iowa L. Rev. 439 (March, 1995)

조에 따르면, “대중은 거주의 자유와 거주지 변경의 자유를 가진다.” 그러므로 누군가의 거주지는 불법적인 침해로부터 보호되어야 한다.[8)]

더욱이, 미국의 9차 헌법 개정[9)]과 같이, 대만 헌법 제22조는 “사회 질서와 공공복지에 유해하지 않은 개인의 모든 자유와 권리는 헌법아래 보장받아야 한다.”라고 명시하고 있다. 1992년, 대 정의 위원회(the Council of Grand Justices)에서 사생활 권리는 처음으로 “대 정의 위원회 293호 토론자의 권리에 대한 해석”이라고 명료하게 명시되었다. 하지만, 대 정의 위원회는 사생활의 권리의 본질을 명확히 하는 점에선 실패했다. 사생활의 권리는 은행법 제48조 2항[10)]에 명시된 점에서 보호되어야 하는 것인가 혹은 헌법 제22조의 헌법에 명시된 기본 권리에 의해 보호돼야 하는 것인가? 반대 의견에서, 대 정의 위원회는 사생활의 권리를 인권의 하위 범주로 간주하고 있다. 이는 민법에 의해 보호받는 권리이자 헌법에 명시된 시민권이다.[11)]

대 정의 위원회 293항의 해석이 사생활의 내용을 상세히 명시하지 않은 점에서 한계가 있다. 대만 은행법에 따라 위 293항의 해석은 고객 개인정보의 보호를 포함하고 있다는 점을 바탕으로 사생활정보는 사생활권리[12)] 종류 중 한가지로 간주되어져야 한다. 나아가, 사생활정보권리는 개인 정보 수집·처리·사용·공유에 대한 통제권 까지를 의미한다.

2005년, “대 정의 위원회 603호, 당사자의 지문 없이 새로운 대만 주민등록증 발급 불가에 관한 쟁점에 대한 해석”이라는 항목으로 사생활정보의 권리가 대 정의 위원회에 처음으로 명확하게 명시되었다. 대 정의 위원회에 따르면, 사생활정보는 “개인이 그들의 개인정보를 발설할지 말지에 관한 권리 혹은 어느 정도로, 어느 기간에, 어떤 방법으로, 어떤 사람에게 정보가 발설될지에 관한 권리를 가지는 점을 보장하는 것”을 의미한다. 더 나아가 위 항목은 각 개인이 그들의 개인정보가 어떻게 사용되어지는지 알고 통제할 수 있는 권리와 그들의 정보에 접근하는 불명확한 정보수집자를 바로잡을 권리를 보장하기 위해 고안되었다.

---

8) 참고 Ying-Fu You, News Media and Press, in ModernState and Constitutional Law, 769-770 (Angle Publishing Co. Ltd., Taipei, March, 1997)

9) 미국 헌법의 제 9차 헌법 개정: “헌법에 명시된 특정 권리는 다른 사람을 해치거나 폄하하는 경우가 아니라면 보호되어야 한다.”

10) 대만 은행법 제48조 2항에 따라, 별도의 법과 규칙이 없으면 은행은 고객의 예금, 대출, 송금액과 관련된 모든 정보를 기밀로 유지해야 한다.

11) 참고 Tzu-Yi Lin, Ji Yin ZiXun Yu Ji Yin Yin Si Quan (Genetic Information and Right to Genetic Privacy), in Dang Dai Gong Fa Xin Lun (New Theory of Contemporary Public Law), Second Volume, 697-703 (Angle Publishing Co. Ltd., Taipei, July, 2002)

12) 참고 id.

2. 무엇이 개인정보인가?

위에 명시되었듯이, 사생활정보 권리는 개인정보의 수집·처리·사용·공유에 대한 통제권으로 명시되었다. 그러므로 사생활정보 권리의 핵심은 "개인 정보"를 어떻게 정의 하냐이다. 클린턴 행정부의 정보기반전담반이 만든 "개인정보의 제공과 사용 원칙"에 따르면, 개인정보는 "개인을 식별할 수 있는 정보"로 정의된다.[13]

개인 정보의 정의는 "정보와 사람사이의 관계를 규정"하는 점으로, 이는 "(1) 개인의 저작권에 대한 관계, (2) 개인에 대한 서술적 관계, (3) 개인에 대한 도구적 관계로 해석되어왔다.[14] 첫째, 개인의 저작권에 대한 관계는 타인과의 소통을 위해 각 개인이 준비한 정보를 개인의 저작물로 연결한다. 이에 따라 전자 메일이나 편지는 개인정보가 된다. 둘째, 개인정보는 성별, 키, 몸무게, 혈액형, DNA, 결혼 상태, 신용 정보, 종교, 정당과 같은 개인의 생물학적이거나 사회적 상태를 말한다. 셋째, 개인정보가 개인을 나타내는 도구임을 분명하게 드러내는 예는 개인의 사회보장번호나 신분번호이다.[15] 신분번호는 기록 관리를 위해 정부에서 개인에게 발급되었다. 개인정보는 글로 명시된 정보부터 사진, 시청각 자료, 녹음 등 각 개인이 죽었든 살았든 관계없이 개인을 식별할 수 있는 정보는 모두 포함한다.[16]

사생활정보의 권리가 개인정보의 불법적인 수집·사용·공유만을 보호하기 때문에, 개인정보가 아닌 정보들은 여전히 보호받지 못하고 있다.[17] 일반적으로 비개인정보는 비인적정보, 익명 정보, 집단 정보 등을 말한다. 비인적 정보란 사람과 관련이 없는 정보이다. 몇몇 익명성 자료는 개인정보로 간주되지 않는다. 하지만 연구 자료나 출판물에서 개인의 신상정보가 노출될 때, 익명의 정보가 개인정보로 분류되어지는 점을 주목해야한다. 집단 정보는 특정 개인이 아니라 집단을 식별하는 정보라면 비개인정보로 간주되어야한다.[18]

개인정보보호법령 제2조 1항 1호에 따르면, 대만에서 개인정보의 정의는 위와 유사하게 통용되고 있다. 개인정보는 이름, 생일, 주민등록번호, 여권번호, 지문, 결혼상태, 가족, 교육, 직

13) 참고 Henry M. Cooper, The Electronic Communications Privacy Act: Does The Answer to The Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis, 20 J. Marshall J. Computer & Info. L. 3 (Fall, 2001)

14) 참고 Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1207 (1998)

15) 참고 id. at 1207-1208.

16) 참고 Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 Ind. L. Rev. 182 (1999).

17) 참고 Henry M. Cooper, The Electronic Communications Privacy Act: Does The Answer to The Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis, 20 J. Marshall J. Computer & Info. L. 3 (Fall, 2001).

18) 참고 id. at 3-4.

업, 진료기록, 유전정보, 성생활, 건강검진, 전과기록, 연락처, 재정상태, 사회활동과 같은 정보들에 그치지 않고 특정인을 식별하기 충분한 정보와 자연인을 직·간접적으로 나타내는 정보를 의미한다.

위의 개인정보의 정의는 가장 기본적인 정의이며 개인정보의 정의는 적용 가능한 법과 규율에 따른다. 예를 들어, 금융지주회사법에 따르면 소비자의 개인 정보는 기본정보, 계좌잔액, 신용, 투자, 보험 정보들로 분류되어진다. 사실상 특정 산업에 대한 이질적인 법규가 목적에 따라 개인정보를 다르게 정의하는 경향이 있다.

3. 개인정보 시장과 시장 실패

정보 경제의 발전과 번영은 대만에 개인정보 시장을 상당하게 활성화하였다. 개인정보는 내부 마케팅과 판매의 목적으로 사용되고 상업 자산으로 널리 여겨지고 있다. 이에 따라 회사의 개인정보 수집·사용·공유 동기는 더욱 강화된다. 현재, 산업계는 소비자의 동의하에 개인정보를 합법적으로 수집·사용·전파하고 있다. 하지만 수백만 명의 개인정보가 이익을 위해 불법적으로 팔리는 경우도 존재하는데, 불법정보수집가가 정부기관 뿐 아니라 금융계, 통신회사와 같은 비정부기관으로부터 개인정보를 수집하여, 텔레마케팅 회사나 사기조직에게 정보를 파는 경우가 해당된다.[19]

더욱 문제가 되는 점은 대만의 개인정보 시장 실패이다. 대만의 개인정보 시장은 외부효과와 높은 거래 비용, 심각한 정보 불균형, 사생활정보의 가격차별의 부재의 결과로 시장실패를 경험하고 있다. 이러한 시장실패를 극복하기 위해서 미국은 자유 시장경제 체제에 집중했지만, 대만정부는 규제적 접근을 채택해야한다. 대만에서 규제책이 존재하였지만, 여전히 맹점은 존재한다. 컴퓨터처리개인정보보호법(the Taiwanese Computer-Processed Personal Data Protection Law, CPPDPL)으로 상대적으로 종합적인 법이 1995년 8월 제정되었고, 지난 20년간 대만의 컴퓨터처리개인정보보호법은 개인정보의 수집·처리·사용·공유에 관한 내용을 12개의 특정 민간산업 분야로 제한하여 적용하였다.[20] 이러한 점에서 12개 산업군 이외의 개인과 타산업군에 의해 수집·사용·공유된 개인 정보는 컴퓨터 처리 개인 정보 보호법(CPPDPL)으로 보호·통제되지 못하고, 즉 이는 대만 개인정보시장에서 대부분의 개인정보가 규제되고 있지 않

19) 참고 Yu-Ming Chang, Wu Bai Wan Bi Ge Ren Zi Liao Bei Dao Mai (Five Million Entries of Personal Information Are Illegally Sold), Taiwan Daily, April 28, 2004

20) 참고 Jeanette Teh, Privacy Wars in Cyberspace: An Examination of the Legal and Business Tensions in Information Privacy, 4 Yale Symp. L. & Tech. 10 (2001/2002).

음을 나타낸다. 더욱이, 민법이나 형법에 의해 보호되지 않는 한, 명시된 12개 산업군 이외의 개인과 산업군은 개인정보를 자유롭게 수집·처리·사용·공유하고 있다. 즉, 명시된 12개 산업군 이외의 개인과 산업계에 의해 생겨난 개인정보 시장은 자유방임시장체제로 간주된다. 하지만 사실상 사생활정보와 관련된 현실에선 자유방임시장 이론인 아담스미스의 보이지 않는 손이란 개념은 실제로 기능하지 않는다.[21] 사기집단이 대만 전역에 걸쳐 소비자 개인정보를 수집하고 오용한다는 점은 보이지 않는 손이 작동하지 않는 것을 명확하게 드러낸다.[22] 사생활정보의 침해가 심각한 현실은 사생활정보를 희소한 자원으로 만들었다. 미국 통운 회사(American Express Company)의 조사에 따르면 25%의 대만인이 개인정보의 오용을 걱정한다고 한다.[23] 다른 설문은 53%의 대만 신용카드 사용자가 은행의 개인정보 보호역량에 대해 회의감을 드러내는 걸로 나타났다.[24] 그러므로 사생활 옹호자들은 개인정보를 효과적으로 보호하기 위해 개인 정보 보호 법률(Personal Data Protection Act)과 같은 더욱 종합적이고 강도 높은 법의 제정 등 정부 개입의 개입을 요구했다.[25] 그 결과로, 개인정보보호법률은 2010년에 통과되었고 2012년에 시행되었다.

4. 개인정보보호를 위한 규제책

헌법과 더불어 다음은 대만의 개인정보 보호를 위한 정부의 규제책들이다.

A. 민법의 사생활 조문

사생활정보는 사생활 권리 중 한 가지 종류이고, 사생활 권리는 인권의 하위범주이다. 그러므로 민법에서 인권을 보호하는 불법행위 조문을 사생활정보에 적용할 수 있다. 민법 제18조 1항과 2항에 따라, 인권이 침해될 때, 개인은 침해를 해결하거나 예방하기 위해 소송을 제기할 수 있다. 또한 민법 제184조 1항에 따르면, “다른 사람의 권리를 의도적으로 혹은 부주의하게 침해한 사람은 피해를 보상해야한다.”라고 명시되어 있다. 법이 개괄적이고 모호하게 명시되어

21) 컴퓨터처리개인정보보호법(CPPDPL) 제3조 1항 6조

22) 참고 Zi-Hsien Chen, Dao Mai Ge ZiBei Su (Being Sued as a result of illegally selling personal information.), Chinatimes Daily, December 22, 2004.

23) 참고 Ti Su, Wang Lu Xin Lai Biao Zhang Dui Xiao FeiZhe Xing Wei Zhi Ying Xiang (The Influence of Internet Trust Mark on Consumer’s Behavior), Electronic Commerce Pilot 2 (July 15, 2004) 접속일 2016년 4월 16일 http://www.ec.org.tw/Htmlupload/6-10.pdf

24) 참고 id.

25) 참고 Yi-Ming Lin, Bao Hu Ge Zi Jian Chi Zui Shao Yuan Ze (Personal Information Protection Requires Minimum Principle), Lihbao Daily, June 9, 2004, at http://publish.lihpao.com/2004/06/09/ (last visited May 22, 2016).

있지만, 제184조에 명시된 보호받을 권리는 인권을 포함한다.[26] 1999년, "사생활"이란 용어는 민법에 처음으로 추가되었다. 개정된 민법 제195조 1항에 명시되길, 신체와 건강, 명성, 자유, 신용, "사생활", 순결, 그 외 다른 이익이 상당히 침해될 때, 피해를 받은 개인은 금전적인 손실이 없더라도 합리적인 금전보상을 요구할 수 있다. 민법의 불법행위 조문 위반에 의거해 개인정보 불법 수집으로 사생활정보를 침해한 정보 수집가들에 대해 개인은 보상을 청구할 수 있다.

B. 형법의 사생활 조문

형법 제317조에 명시되길 "자신의 사업을 위해 타인의 비밀을 상업적이거나 업무적으로 보관하거나 적법한 이유 없이 누군가의 비밀을 발설한 사람은 약 일 년의 징역이나 구금, 약 1000위안의 벌금형에 처한다." 또한 형법 제318-1조에는 "컴퓨터나 다른 장비에 저장되어 있는 타인의 비밀을 이유 없이 발설하는 사람은 약 2년의 징역, 구금, 약 5000위안의 벌금형에 처한다."라고 명시되어있다. 위의 두 조항은 소비자의 기밀 개인 정보를 불법적으로 발설한 정보 수집가들에게 적용될 수 있다.

C. 개인 정보 보호 법령

최근, 개인정보를 보호하기 위해 개인정보법령이 정부기관이나 민간 업체를 통해 이루어진 개인정보 수집·처리·사용·공유에 광범위하고 포괄적으로 적용되고 있다. 하지만 대만의 법규는 단일 사생활위원회를 만드는 대부분의 유럽의 모델과는 다르다. 사생활 규제에 관련 모든 기관이 법무부에 소속되어 있음에도 불구하고, 특정 산업계를 담당하는 수많은 전문 기관들이 개인 정보 보호 법령을 시행하고 있다.[27] 다음은 개인정보보호법령의 주요 조항인데, 이는 OECD의 사생활 8대 원칙[28]과 관계가 있다.

---

26) 참고 Ying-Fu You, News Media and Press, in Modern State and Constitutional Law, 773 (Angle Publishing Co. Ltd., Taipei, March, 1997).

27) 참고 Fred Chilton ET AL., 1996 Computer and Telecommunications Law Update New Developments: Asia Pacific, 15 J. Marshall J. Computer & Info. L. 125 (Fall, 1996).

28) OECD는 수집의 제한, 정보 정확성, 목적의 구체성, 사용의 제한, 안정성 확보, 공개, 개인의 참여, 투명성, 책임성을 사생활 8대 원칙으로 명시하였다. 참고 Jody R. Westby, American Bar Association, International Guide to Privacy 84-85 (2004).

(1) 수집제한의 원칙

개인정보보호법령 제15조 2항 1호와 제19조 5항 1호에 의하면, 관련 개인의 동의 없이 개인정보를 수집할 수 없다. 또한 개인정보보호법령 제8조와 제9조에 명시되길, 공·사조직은 개인정보가 어떻게 수집·처리·사용·공유되는지와 그 목적에 관해 당사자에게 적절하게 알릴 의무가 있다. 그러므로 공·사조직은 개개인에게 정확하고 충분한 설명을 하면서 당사자의 동의를 구하기 위해 개인정보의 수집··사용·공유의 목적을 당사자에게 설명하여야 한다.

(2) 정보 정확성의 원칙

개인정보보호법령 제15조 제19조에 따르면, 수집된 개인정보는 사용 목적에 맞게 관계가 있어야 한다. 개인정보보호법령 제11조 1항에 따르면 정보 수집가는 개인정보의 정확성을 유지해야하고 의무에 준거하거나 관련 개인의 요청에 따라 개인 정보를 정정하거나 보충하여야 한다.

(3) 목적 구체성의 원칙

개인정보보호법령 제15조와 제19조에 따르면, 개인정보의 수집·사용·전파 목적은 구체적이어야 한다. 법무부는 중앙관할관청과 함께 각 산업군을 담당하여 개인정보를 분류하고 목적의 범주를 규정해야한다. 그러나, 특정한 목적의 범위가 광범위하게 정의된 산업에서는 정보수집가들이 개인정보 수집·처리·사용·전파에 더욱 큰 자유가 있고, 이에 피해를 받는 개인은 그들의 개인정보에 관한 권리에 더욱 제한이 있다.[29)]

(4) 사용 제한의 원칙

개인정보보호법령 제16조와 제20조에 따라, 개인정보는 법이나 당사자의 동의가 없다면 처음 수집 목적에 따라서 사용되어야 한다.

(5) 안전성 확보의 원칙

개인정보보호법령 제6조와 제18조, 제27조에 따르면, 정보 수집가는 개인정보가 도난·변형·손상·파손·발설되는 경우를 대비해 안정성 확보 계획을 가지고 있어야 한다. 또한 개인정보보호법령의 시행 규칙 제12조에 따르면, 정보를 수집하는 공·사조직은 개인정보의 도난·변형·손상·파

29) 참고 Wen-yi Hsu, Ge Ren Zi Liao Bao Hu Fa Lun (On Personal Information Protection) 184 (Sanmin Publishing Co. Ltd., Taipei, November, 2001).

손·발설을 방지할 목적으로 적절한 기술과 체계적 방법을 수립해야 한다.

⑹ 공개의 원칙

개인정보보호법령 제17조에 따르면, 정부 기관에 저장된 개인정보 파일에 관해 기관은 이름과 분류, 파일의 범위, 정부기관에 의한 파일의 유지와 사용, 개인정보 수집의 수단 등의 내용을 공개하여야한다.

⑺ 개인 참여의 원칙

개인정보보호법령 제3조, 제10조, 제11조에 따르면, 개인은 개인정보의 정확성에 관한 논란에 대하여 수집되어 보관중인 자신의 개인정보에 관해 문의하고 검토, 사본 제작, 수정, 보충할 수 있는 권리를 가진다. 이는 개인이 자신의 개인정보 수집·처리·사용·전파의 중지를 요청할 수 있도록 하기 위함이다.

⑻ 책임의 원칙

개인정보보호법령을 위반하여 개인의 권리와 이익을 침해한 공·사조직의 정보 수집가는 그로부터 발생한 손해에 대한 책임이 있다. 개인정보보호법령 제28조 3항, 제29조 2항에 따라, 정보 수집가로 인해 발생한 손해에 대하여 피해자가 실제 피해 금액에 대한 증거를 제출하지 못하는 피해사건의 경우엔 총 보상액은 각각의 손해 사건에 대해 인당 500 대만달러(약 한화 2만원) 이상 20,000 대만달러(약 한화 70만원)이하이다. 하지만, 개인 정보 보호 법령 제28조 2항과 29조 2항에 따르면, 한 사건으로 인해 발생한 손해에 관하여 관련된 사람들에게 정보 수집가가 보상해야하는 총 보상 금액은 2천 대만달러(약 한화 7억) 이상 2억 대만달러(약 한화 72억) 이하로 보상금액이 증가한다.

또한, 개인정보보호법령 제42조에 따르면, 자신이나 타인으로부터 부당이득을 취할 의도가 있거나, 불법적으로 개인정보 파일을 변형 혹은 삭제하여 타인의 이익을 침해할 의도가 있거나, 불법적인 수단으로 타인의 개인정보 파일의 정확성을 손상시키고 타인에게 손해를 끼친 개인 정보 수집가는 5년 이하의 징역·구금이나, 백만 대만달러 이하의 벌금형, 혹은 위 두 징역과 벌금에 처한다.

현재의 개인정보보호법령이 2012년 10월 시행되기 이전에, 현재 개인정보보호법령의 전신인 대만의 컴퓨터처리개인정보보호법(CPPDPL)의 조항을 위반하여 개인의 권리와 이익을 침해한 정보수집자는 그로부터 발생한 손해를 책임져야했다. 컴퓨터처리개인정보보호법 하에서, 정보

수집가로 인해 발생한 손해에 대하여 피해자가 실제 피해 금액에 대한 증거를 제출하지 못한 피해사건의 경우의 총 보상 금액은 2만 대만달러(약 한화 72만원) 이상 10만 대만달러(약 한화 364만원) 이하였다. 이는 위의 개인정보보호법령에 명시된 벌금보다 더욱 큰 액수이다. 한 사건으로 인해 발생한 손해에 대하여 관련된 사람들에게 정보 수집가가 보상해야하는 총 보상 금액은 2천 대만달러(약 한화 7억원)를 넘지 못한다. 하지만 하나의 불법 개인정보 자료파일이 백만 명 이상의 개인정보를 포함하고 있는 상황에서 총 보상 금액을 제한하면, 개인에게 돌아가는 보상금액은 20 대만달러(한화 700원) 보다도 작다.[30] 그 결과로 피해를 당한 개개인은 개인정보 보호조항과 계약 이행을 하지 않는 정보수집가들을 감시할만한 동기를 잃게 된다.

2012년 10월 1일부터 사생활정보를 효과적으로 보호하기 위해, 개인정보의 권리를 이행할 개인의 동기를 증진하기 위해 보상액의 상한선을 없애거나 인상하였다. 또한 현행 개인정보보호법령에 소비자 보호 집단이 소비자의 권리를 대신하여 소송할 수 있는 권리를 가진 경우엔 집단소송 방법이 소개되었다. 나아가 대만 소비자보호법(Taiwanese Consumer Protection Law)[31]과 같이 앞으로는 처벌적 손해 배상금도 개인정보보호법령에 도입될 수 있을 것이다. 고의의 위법행위에 의거한 손해가 생긴 경우 처벌적 손해배상금으로 정보 수집가는 실제 손해액의 세배까지 청구될 수 있을 것이며, 과실에 의한 손해의 경우엔 실제 피해 금액만큼의 손해배상금이 청구될 수 있을 것이다.

개인정보보호법률 또는 다른 적용 가능한 법 하에서 법적책임을 다루기 위해 대만 은행법은 개인정보 유출사건으로부터 생기는 법적책임을 최대 이천만 대만달러(약 7억 원)까지 보장하는 새로운 보험 정책을 제안한다.[32] 하지만 보험은 피보험자에서 보험회사로 위험을 전가하는 것이므로, 피보험자는 더욱 위험한 행동을 할 수 있다. 위험이 보험회사로 전가되기 때문에 피보험자가 사생활 범죄 예방책을 줄일 유인이 증가한다. 한편 도덕적 해이로 인해 보험회사 측에서도 보험을 위한 예방책들을 줄이려고 한다. 보험 회사가 공동보험과 공제제도, 경험 요정법 등 도덕적 해이를 줄일 수 있는 다양한 방법을 사용하지만,[33] 이러한 노력에도 불구하고 보험으로 모든 책무를 변제하려는 대만 은행법 하에선, “피보험자는 사건이 발생하지 않던 발생해

30) 참고 Yu-Ting Chen, Ge Zi Wai Xie Yin Hang XunQiuBao Hu (Banks Seek Protection as a Result of Personal Information Leakage), Chinatimes Daily, October 28, 2004.

31) 대만소비자보호법 제51조에 따르면, 이 법과 연관된 소송에서, 고의의 위법행위에 의거한 손해가 생긴 경우 피해 입은 소비자는 처벌적 손해 배상금을 실제 피해액에 총 세배까지 청구할 수 있다. 과실에 의한 손해의 경우엔 실제 피해 금액만큼의 손해배상금이 청구될 수 있을 것이다.

32) 참고 Yu-Ting Chen, Ge Zi Wai Xie Yin Hang Xun Qiu Bao Hu (Banks Seek Protection as a Result of Personal Information Leakage), Chinatimes Daily, October 28, 2004.

33) 참고 Robert Cooter & Thomas Ulen, Law and Economics 354-355 (4th ed. 2004).

서 고소를 당하든 관계가 없게 되는" "전액보장 보험"을 가진다.[34] 이에 따라 피보험자는 사고에 대해 신경 쓰지 않게 된다. 그러므로 피보험자는 권한 없는 접속, 사용, 유출 으로부터 개인 정보를 보호할 안정망 구축과 실시할 유인을 잃게 된다. 이러한 점에서 소비자의 개인정보를 보호하기 위해서는 은행법이 제안한 전액보장 보험 정책은 시행되어지면 안 되고 공동보험, 공제제도 등으로 대체되어야 한다.

(9) 개인정보의 국제 전파에 대한 제한

정부기관에 의한 개인정보의 국제적 전파는 관련법과 규율에 따른다. 사기업에 의한 개인정보의 국제 전파에 관해 말하자면, 법무부와 같은 관할관청이 이러한 국제 전파를 다음과 같은 상황에서 제한할 수 있다. 1) 정보를 받는 국가가 적절한 수준의 사생활정보 보호를 하지 않아 자료에 손상을 끼칠 염려가 있을 경우이다. 또한 2) 개인정보보호법령 제21조에 따르면 개인정보가 제 3국으로 전송되어 적용 가능한 법을 회피할 수 있는 수단으로 사용될 수 있는 경우이다.

EU자료보호령(EU Data Protection Directive)과 같이 개인정보보호법령은 일정 수준의 적정한 사생활정보 보호가 결여된 대만에서 제 3국으로의 자료의 이전을 금지한다. 하지만, 컴퓨터와 기술의 발전이 사실상 개인정보 유출의 탐지와 통제를 어렵게하고 이에 관련된 비용의 상승 때문에, 개인정보들이 사실상 불법적으로 대만의 내 외에서 널리 퍼지고 있다.

5. 개인 정보 보호의 비용

사생활정보는 개인을 정의하는 개인의 권리를 보호하는데 중점을 두고 있다.[35] 개인 특징의 내 외적 주안점은 개인의 정체성을 형성하는데 있어 필수적이다. 사생활정보의 보호가 현대 사회에서 개인의 삶의 질에 필수적일 지라도, 사생활을 허용하는 점에 실질비용이 부과된다는 점은 명백하다. "개인에 대한 정보가 타인에게 언제, 어떻게, 어느 정도까지 공개될지를 결정하는 개인과 집단, 기관에 대한 주장"을 위한 법적 보호 하에선 오해의 여지가 있다.[36] 사생활정보가 개인의 사생활에 관한 점이라 그와 관련된 거짓말의 탐지가 어렵고 사실상 불가능하기에 사생활정보는 부정확한 정보의 전파를 촉진한다. 예를 들면, 취업 희망자는 자신의 경력에 대

34) 참고 id. at 355.

35) 참고 Richard C. Turkington, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. Ill. U. L. Rev. 479 (1990).

36) 참고 Alan F. Westin, Privacy and Freedom 7 (1967).

해서 속일수도 있다. 이와 마찬가지로, 사생활정보는 관련된 옳은 정보의 공유를 차단한다. 예를 들어, 기장이 일에 영향을 끼칠 수 있는 그의 나쁜 건강상태를 보고하지 않으면, 이는 소비자의 안전을 위협할지도 모른다. 정부와 기업, 다른 단체가 신속하고 정보에 기반을 둔 의사결정을 위해 구축한 개인 정보와 이의 수집·처리·사용·공유는 사생활정보라는 이름하에 제한될 수 있다. 이러한 점에서 사생활정보를 유지하는 비용은 크다. 이는 그들이 수집한 정보의 정확성과 완전성을 확인하려하는 정보 사용자에게 거래 비용을 발생시키고, 부정확하고 불완전한 정보로 인한 미래 위험부담 때문에 비용이 증가한다. 즉, 사생활정보는 생산성을 줄이고 더욱 값비싼 서비스와 재화를 만든다.[37]

그러므로 사생활정보 비용이나 그 가치가 완전하지 않다는 점은 명백하다. 한 개인의 사생활정보 이권은 타인 혹은 사회의 이익과 상충될 수 있다. 이 두 이익 사이에서 균형을 맞추는 것이 중요하다.[38] 다양성과 문맥적 맥락의 중요성, 대중과 상업적 이익, 정직함과 같은 경쟁적 가치를 고려하지 못한다면, 사생활정보 보호는 불가능하다.

Ⅲ. 대만의 국가 신분 카드 번호의 발전과 규제

사생활정보는 정부와 기업, 다른 조직이 신속하고 정보에 기반을 둔 결정을 하는데 필수적인 개인정보의 수집·처리·사용·공유를 제한한다. 하지만 각 개인이 점점 더 증가하고 커져가는 매일의 재화, 서비스, 활동을 포기하려는 것이 아니라면 한사람의 신분을 증명하는 개인정보를 수집하는 정보수집가를 줄이는 것은 바람직한 방법이 아니다. 현대사회에서 각 개인은 신용카드 번호, 은행 계좌번호, 핸드폰번로, 운전면허증, 클럽회원권, 학생증번호 등등의 다양한 특정 목적을 위해 자신의 개인정보를 발설하고 이는 이러한 신분확인은 자료를 바탕으로 이루어진다. 이와 유사하게 국가신분증과 주민등록번호는 개인을 식별하기 위해 정부가 발급하였다.

대만을 포함한 100여 개국 이상이 신분증과 주민등록 체계를 가지고 있다. 국가신분체제는 개인정보에 관한 자료를 주민등록번호와 같은 식별체와 연결하여 각 개인이 쉽게 자료와 연결되도록 하는데 의의가 있다. 국가신분체계의 지지자는 효율성, 접속용이, 사기방지, 범죄와 테러 검열 등을 이유로 신분체계를 지지한다. 하지만 비판자들은 신분증 또는 주민등록번호 분실, 도난, 남용 시 국가신분체계가 사생활을 침해할 위험[39]을 증가시키고 있다고 주장한다. 다

37) 참고 Fred H. Cate, Privacy in the Information Age 28-29 (1997).
38) 참고 id.

음은 대만의 주민등록번호의 발전과 관련 규제책이다.

1. 국가 신분 카드 번호의 세대와 출범과 배정

대만의 주민등록번호는 개인을 식별하기 위해 사용되고 있고 이는 전국에서 효력이 있다.[40] 각 시민들은 국가신분증을 만들 자격이 있다. 개인은 14살이 되면 처음으로 국가신분증을 만들도록 되어있다.[41] 게다가 14살 이하도 국가 신분증을 요청할 수 있다.[42] 국가 신분증을 만들기 위해 신분증 사진이 제시되어야 한다.[43] 만약 개인의 국가 신분증이 파손 또는 분실된다면, 개인은 재발급을 신청해야 한다.[44] 개인이 호적을 등록하여 국가신분증 정보가 바뀔 시에는, 각 개인은 국가 신분증의 갱신을 요청해야한다.[45] 각 개인은 항상 국가신분증을 소지하여야 한다. 법에 의하지 않고서는, 국가신분증은 압수될 수 없다.[46]

각 개인은 호적사무소에서 주민등록번호를 생일과 호적, 귀화에 근거해 할당받게 된다.[47] 12살 이하의 각 개인은 출생신고의 대상이다.[48] 출생신고는 출생 후 60일 이내에 부모, 조부모, 호주, 동거인, 양부모가 신고해야 한다.[49]

주민등록번호는 순서대로 부여되고, 중복되거나 실수가 있는 경우에는 호적사무소에서 정정되거나 대체되어진다.[50] 과거에는 국가신분증에 포함된 개인 정보가 수기로 작성되었다. 이 연유로 한 개인이 타인과 같은 번호를 가지게 되어 쥬민등록번호가 겹치는 일이 많았다. 하지만 다른 등기사무소와 컴퓨터를 사용한 내부망이 생기면서 신분번호가 겹치는 일은 거의 발생하지 않고 있다. 각 개인이 고유한 주민등록번호를 할당받으면서, 각 개인은 타인으로부터 구별되는 주민등록번호를 부여받았다. 주민등록번호는 1자리의 영문 알파벳과 9자리의 숫자로 이루어진 10자리의 코드로 이루어졌다. 첫 번째 영문 알파벳은 출생신고를 한 대만의 22개의 지역 중 한 지방정부를 나타낸다. 그리고 2번째 숫자는 성별을, 10번째 숫자는 검사 코드를 나타낸

39) 참고 Daniel J. Solove and Marc Rotenberg, Information Privacy Law 454-455 (2003).
40) 호적법(戶籍法), 제51조
41) 호적법(戶籍法), 제57조
42) 호적법(戶籍法), 제57조
43) 국민 신분증와 호적을 위한 사진 파일에 대한 정부 규칙(國民身分證及戶口名簿製發相片影像檔建置管理辦法) 제10조
44) 호적법(戶籍法), 제57조
45) 호적법(戶籍法), 제58조
46) 호적법(戶籍法), 제56조
47) 국민 신분증와 호적을 위한 사진 파일에 대한 정부 규칙(國民身分證及戶口名簿製發相片影像檔建置管理辦法) 제6조 1항
48) 호적법(戶籍法), 제6조
49) 호적법(戶籍法), 제29조, 제48조
50) 국민 신분증와 호적을 위한 사진 파일에 대한 정부 규칙(國民身分證及戶口名簿製發相片影像檔建置管理辦法) 제7조

다.[51] 예를 들어 출생신고 장소를 좀 더 설명하자면, 알파벳 "A"는 대만의 수도 타이베이를, "B"는 대만의 중부 대중(Taichung)시를 "E"는 남서부 도시 가오슝(Kaohsiung)을 나타낸다. 성별코드는 "1"은 남성을 "2"는 여성을 가리킨다. 한국의 시스템과 다르게 대만신분증 번호 체계는 신분증 소지자의 생일과 같은 개인적 특성이나 정보를 직접적으로 나타내지 않는다. 하지만 신분증 번호는 여전히 성별과 출생지과 같은 신분증 번호 소지자의 개인정보를 담고 있기는 하다.

(신분증 견본 앞면)

(신분증 견본 뒷면)

2. 주민등록번호의 간략한 역사

1965년 이전, 대만은 국가신분증을 시민에게 발급하였으나 주민등록번호 체계는 아직 도입되지 않았다. 1965년, 정부는 국가신분증에 새로운 전환기를 맞아 신분증 소지자에게 일련번호를 할당하기 시작했다. 1965년 4월 17일, 대만의 양밍산 행정구는 장제스 대통령에게 그의 주민등록번호 - Y10000001 - 가 적힌, 새로 개정된 형태 중의 하나인 국가신분증을 발급했다. 당시의 주민등록번호는 9자리로써 마지막 한 자리의 검사 코드가 없었다. 1969년 이후, 주민등록번호 체계에 컴퓨터 처리로 인한 검사 코드가 추가되었고, 시민들은 즉각적으로 출생신고에 기반을 두어 주민등록번호를 할당받았다.[52]

3. "지문 없이 발급되지 않는 새로운 주민등록증"의 헌법 위반

호적법 제8-2조와 8-3조의 관련 조항에 관해 대만의 새로운 신분증이 지문 없이는 발행

51) 국민 신분증와 호적을 위한 사진 파일에 대한 정부 규칙(國民身分證及戶口名簿製發相片影像檔建置管理辦法) 제5조
52) 국가 신분증의 발전.
https://zh.wikipedia.org/wiki/%E4%B8%AD%E8%8F%AF%E6%B0%91%E5%9C%8B%E5%9C%8B%E6%B0%91%E8%BA%AB%E5%88%86%E8%AD%89.

4.