

전자주민증과 정보인권

* 전남대학교 공익인권법센터 「인권법평론」 2011 제7호 게재

장여경¹⁾

I. 들어가며

정부는 지난 해 9월 전자주민증 도입을 내용으로 한 주민등록법 일부개정법률안²⁾을 발의하였다. 1998년 김대중 정부의 등장과 더불어 전자주민카드 계획이 백지화된 이후로 12년 만에 국가신분증의 전자화가 본격적으로 추진되는 것이다. 국회 상임위원회는 여러 차례 제안된 수정안들을 검토하며 이 법안을 심사 중이다³⁾.

대한민국 국민들에게 전자주민증의 문제는 미완의 민주주의 문제이기도 하다. 멀리는 일제강점기와 미군정의 역사 속에서, 가까이는 군사독재정권 치하에서 도입된 주민등록제도의 반민주성과 인권침해 문제가 현재까지 시정 없이 계속되어 왔다⁴⁾. 한국의 주민등록제도는 복지를 위한 목적이 아니라 국민을 효과적으로 관리하고자 하는 필요성에 의해 도입되었다는 데에 그 특이성이 있다(조화순, 2005). 주민등록제도와 정보 기술의 결합은 시민권을 압도하는 국가와 기업의 권한을 확대시키고 있다.

1998년 전자주민카드는, 최초의 평화적인 정권 교체를 이루어낸 시민의 힘으로, 당시로서는 상당히 선진적이었던 ‘프라이버시’의 권리 프레임을 성공적으로 제기함으로써 저지되었다(임현만, 2005). 전자주민카드와 관련한 당시 논의에는 카드가 정보주체인 개인의 이익에 반하여 개인의 정보프라이버시를 침해할 것이라는 인식과 국가와 조직의 권력을 증대시켜 국민의 참여나 대의제적인 정부보다는 기술에 의하여 도움을 받는 관료제적 지배가 될 것이라는 인식이 근간에 있었다(조화순, 2005). 그러나 정권 교체 속에서도 주민등록제도의 개혁은 이루어지지 않았다. 전자주민카드 반대운동은 1999년 십지지문 강제날인제도에 대한 헌법소원과 대중운동으로 맥을 잇는 듯하였으나, 2005년 헌법재판소의 합헌 결정 이후 대중운동도 잦아들었다.

그래서 ‘돌아온 전자주민증’을 바라보는 심경이 복잡할 수밖에 없다. 우리는 미루어 두었던 질문에 답해야 한다. 국가신분증이란 국민에게 무엇인가. 국민은 국가신분증 제

1) 진보네트워킹센터 활동가.

2) 2010. 9. 20. 의안번호 9418.

3) 개정안에 대한 이 수정안들의 법적 지위는 불분명하다. 그러나 정부 발의 법안의 국회 심사 과정에서 정부가 수정 법률안을 제시하는 경우가 다수 있으며, 전자주민증 관련해서는 2011. 7. 현재까지 국회 행정안전위원회에 최소 2차례의 수정안이 제안되었다(행정안전부, 2010c; 2011b). 이 글은 공개된 법안 뿐 아니라 수정안의 내용도 함께 분석의 대상으로 삼았다. 개정안과 수정안 조문 대비표(행정안전부, 2011e)는 일반에 공개된 바 없기에 별첨하였다.

4) “국가권력의 민주적 성립이나 법적 통제가 불충분하였던 박정희정권 하에서 추진된 주민등록, 주민등록증, 주민등록번호, 지문날인 그 자체가 많은 문제점을 갖고 있음에도 불구하고 그동안 이를 헌법상 거의 다루어지지 못한 상태 하에서 이제 이러한 것들이 정보사회에서 ‘새로운’ 기본권침해의 중요수단으로 부각, 활용되고 있다”(김일환, 2005; 김주영, 2011 참조).

도를 어디까지 용인해야 하는가. 이와 같은 근본적인 질문을 던지는 것이 너무 늦은 것은 아닌가. 2005년 헌법재판소의 합헌 결정이 있었고 기왕에 국가신분증이 일상생활에 필수적인 제도로 자리잡아왔으니, 선택지는 제한적이지 않을까. 그나마 우리가 건질 수 있는 이득은 국가신분증의 위·변조와 유출의 위험성을 방지한다는 실용적 관점에서 찾을 수 있지 않을까. 정보인권은 이러한 논쟁에서 어떠한 관점을 제시해야 하는가. 이미 3천 5백만 개의 주민등록번호가 유출된 상황에서 한국은 전자주민증을 실시하면서 충분히 국민의 정보인권을 보호할 수 있을까?

이 글은 현재 국회에서 심사 중인 전자주민증의 쟁점사항을 정보인권의 관점에서 검토하고, 이러한 질문들에 대한 답변을 더불어 찾아보고자 한다.

II. 정보인권의 내용

1. 정보인권 개념의 유래

2003년 유엔이 개최하고 국제통신연합(ITU)이 주최한 정보사회 세계정상회의(World Summit on the Information Society)⁵⁾ 전후로 국제적으로 ‘정보 사회의 인권’의 의미를 밝히는 시도가 활발히 시도되어 왔고, 정보인권(Human Rights in the Digital Age)은 현대 정보화 사회 혹은 디지털 사회에서 인류 문명 발달의 핵심인 의사소통의 자유를 보장하는 4세대 인권으로 규정되어 왔다. 학계에서는 자유민주주의적 가치 내에서 개인 및 사회의 정보에 대한 자유를 보장하기 위한 권리로서 정보인권(citizens' right to information)에 대한 고찰이 있어 온 이래, ‘정보가 수집·가공·유통·활용되는 과정과 그 결과로 얻어진 정보가치에 따라 인간의 존엄성이 훼손되지 않고 이를 통해 삶의 조건이 개선될 수 있도록 하는 최소한의 권리’를 정보인권으로 정의한다(이민영, 2010). 혹은, 헌법상 정보 질서를 구현하기 위하여 ‘정보의 자유’(공적 정보의 자유)와 ‘정보 프라이버시’(사적 정보의 보호)를 통해 국민 개개인이 정보유통에 대한 통제력을 지니게 되는 권리라고 정보인권을 정의하기도 한다(이인호, 2009). 한국 사회에서 이 용어는 2003년 교육행정정보시스템(NEIS) 논쟁 이후 ‘개인정보 자기결정권’을 의미하는 것으로 대중적으로 알려져 왔다⁶⁾.

2. 개인정보 자기결정권의 내용

헌법재판소는 2005년 지문날인 제도에 대한 결정에서 개인정보 자기결정권에 대하여 “자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.”고 실시한 바 있다⁷⁾.

5) <http://www.itu.int/wsisis>

6) 이 글에서는 개인정보 자기결정권의 의미에 특화하여 ‘정보인권’이라는 용어를 사용한다.

비록 헌법재판소는 이 결정에서 주민등록법상 지문날인 제도와 경찰청장이 지문 정보를 보관·전산화하고 이를 범죄수사목적에 이용하는 행위에 대하여 합헌으로 결정하였으나, 결정문은 정보인권과 관련하여 주목할 만한 서술을 다수 포함하고 있다.

먼저 헌법재판소는 “[컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서] 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다”고 경고하며, “이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치”라고 지적하였다. 즉, 개인정보자기결정권은 개인에게 자신에 관한 정보의 공개와 이용에 대하여 원칙적으로 스스로 결정할 권한을 보장하고 있으며, 현대적인 정보처리기술의 조건 아래서는 국가 등 공권력에 의한 개인정보의 무제한적 수집, 저장, 이용 및 교부에 대하여 개인을 보호할 것이 요구된다는 것이다.

개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당함이 분명하다. 따라서 개인정보 자기결정권을 제한하는 법률은 법률유보의 원칙, 과잉금지의 원칙에 의해 엄격히 심사되어야 마땅하다. 특히 헌법재판소는 대상 사건에 대하여 합헌 결정을 내리면서도, 개인정보의 보관·전산화·이용의 주체, 목적, 대상 및 범위 등을 법률에 구체적으로 규정함으로써 그 법률적 근거를 보다 명확히 하는 것이 바람직하다는 의견을 피력하였다.

한편, 헌법재판소는 위 결정에서 국민의 프라이버시권을 침해할 우려가 있고 막대한 비용을 필요로 한다는 이유로 전자주민카드사업이 보류되었다는 사실을 기술하고 있다. 현재 논의 중인 전자주민증 역시 이러한 사유에 저촉되지 않는지 검토할 필요가 있다. 여기서 주목할 점은 헌법재판소가 컴퓨터에 의하여 처리되는 개인정보가 일반문서에 의한 개인정보의 경우에 비하여 기본권침해의 우려가 훨씬 크다는 점을 인정하였다는 사실이다⁸⁾. 즉 기존에 육안 식별 등의 방식에 의존하던 주민등록증 정보의 처리가 전산화되어 컴퓨터에 의하여 처리되는 것은 그 기본권 침해의 정도가 더욱 중대해진다는 사실을 의미한다.

그리고 헌법재판소는 지문 정보를 범죄수사활동, 대형사건사고나 변사자가 발생한 경우의 신원확인, 타인의 인적사항 도용 방지 등 각종 신원확인의 목적을 위하여 이용하였을 때의 공익이 그로 인한 정보주체의 불이익에 비하여 더 크다고 보았다. 즉 지문

7) 현재 2005. 5. 26. 선고, 99헌마513, 2004헌마190(병합).

8) “현대의 정보통신기술의 발달은 그 그림자도 짙게 드리우고 있다. 특히 컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서 개인정보의 처리와 이용이 시공에 구애됨이 없이 간편하고 신속하게 이루어질 수 있게 되었고, 정보처리의 자동화와 정보파일의 결합을 통하여 여러 기관간의 정보교환이 쉬워짐에 따라 한 기관이 보유하고 있는 개인정보를 모든 기관이 동시에 활용하는 것이 가능하게 되었다.”(위 결정문)

정보를 공익적 목적을 위해서가 아니라 상업적인 식별용으로 널리 사용하고 국가가 그러한 계기를 적극적으로 제공한다면, 기본권 침해성은 커질 수 있다. 특히 재판관 송인준, 재판관 주선회, 재판관 전효숙의 반대의견에서는 지문 정보의 민감성을 다음과 같이 힘주어 지적하였다. 첫째, 지문은 개인정보의 연결자로 사용될 수 있다. 국가나 기업, 개인이 지문 정보를 집적하고, 이를 통하여 개인의 성향이나 취미, 소비행태, 병력 등 사생활을 엿볼 수 있으며, 그 개인에 대한 평가, 분석을 함부로 할 수 있어 개인의 사생활의 자유가 침해될 소지가 크다는 것이다. 둘째, 지문은 개인의 신체의 일부분으로 언제 어디서나 남겨두고 다니고 있다. 따라서 국가나 기업, 타인이 그 개인의 행위나 사생활을 추적할 수 있는 여지가 있고, 그 가능성이 알려지거나 스스로 인식하게 되는 경우 개인의 일반적 행동의 자유에 제약을 가져오는 등 개인의 인격과 자유는 심히 위축될 여지가 있다. 때문에 헌법상 개인의 자유와 권리를 최대한으로 보장하기 위하여서는 지문 정보의 수집, 보관, 활용에 대하여 그 목적·대상·범위·기한 등의 요건을 엄격하게 법률로 규율할 필요가 있다. 결국, 지문 정보에 대한 헌법적 보호의 필요성은 지문 정보의 고유성과 동일성으로 인한 식별성과 더불어, 추적가능성 때문이다. 지문 정보의 민감성이란, 뒤에서 살펴볼 정부의 주장대로, 육안으로 지문 정보를 보이거나 보이지 않게 하는 차원의 문제가 아닌 것이다.

컴퓨터나 전산망 등을 통한 개인사생활감시와 개인정보침해는 언제, 어디서 무엇이 얼마만큼 침해되고 있는지를 전혀 또는 거의 모르고 있다가 침해되었다는 사실을 알게 되면 그 구제가 사실상 거의 불가능하다는 특징을 갖고 있다(김일환, 2005). 무엇보다 오늘날 개인정보 수집과 처리를 위한 공공정보시스템은 갈수록 막대한 자원이 투입되는 거대 기술 구조물이기 때문에, 도입 이후 개인정보 자기결정권이 침해되는 상황이 발생한다 하더라도 이를 중단시키기가 어렵다. 따라서 그 침해성을 최소화하기 위하여 사전에 영향평가를 제도화할 것이 요구되고 있다⁹⁾. 이러한 영향평가에서 고려해야 할 점은, 개인정보의 보관·전산화·이용의 주체, 목적, 대상 및 범위 등이 법적으로 근거를 가지고 있는지, 기술적으로 개인정보 보호 원칙¹⁰⁾의 구현이 보장되는지에 관한 것이다.

9) 개인정보보호법(2011. 9. 30 시행) 제33조.

10) OECD 8원칙 등 개인정보보호의 원칙은 기본권보장의 체계에서 볼 때 비례원칙의 구체화 내지 비례원칙의 파생원칙으로 이해될 수 있다. 개인정보보호의 원칙을 기초로 하여 자기정보통제권의 제한에 있어서 준수되어야 할 특수한 요청들을 상정해본다면, 1)목적구속의 원칙 2)수집제한의 원칙 3)정확성·안전성의 원칙 4)정보분리의 원칙 5)시스템공개의 원칙 6)익명성의 원칙을 들 수 있다(권건보, 2005); 그밖에 개인정보보호법 제3조(개인정보 보호 원칙)에서는 다음과 같은 원칙을 제시하였다. ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다. ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다. ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다. ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다. ⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다. ⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다. ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준

특히 공공정보시스템의 구축 및 운용에 있어서는 목적구속원칙을 유념해야 한다. 개인 정보 보호 원칙 중 목적구속원칙은 정보처리목적을 확정하고 다른 한편은 정보처리의 범위를 한정한다. 필요한 최소한도로 사전에 명백하게 규정된 목적을 위한 정보처리만이 허용된다(김일환, 2005). 따라서 개인정보 수집 단계에서부터 그 목적을 명확히 한정하고, 개인정보의 처리 방법 및 종류에 있어서 목적 내 필요 최소한의 개인정보를 수집하고 이용하도록 한정하며, 목적 외 이용을 제한할 수 있는 법적·기술적 조치가 준비되어 있어야 하는 것이다¹¹⁾.

전자신분증에 사용되는 IC칩은 기본적으로 기술적인 확장성이 있다는 점에서 목적구속의 원칙에 의거한 엄격한 검토가 필요하다. 결론적으로 필자는 우리의 전자주민증이 이런 요건을 갖추었는지에 대하여 회의적으로 평가한다.

III. 전자주민증의 도입 내용

1. 도입의 필요성

정부는 전자주민증의 도입 필요성에 대하여 다음과 같이 밝히고 있다(국회 행정안전위원회 수석전문위원, 2010; 행정안전부, 2011c).

첫째, 현 주민등록증 경신 후 10년이 지나 주민등록증의 경신이 필요하다. 구체적으로는 사진이 낡고 용모변화가 심하여 생긴 신분확인업무의 어려움을 해소하고, 새주소 도입을 위해 주민등록증을 교체해야 한다. 개인정보 보호를 위하여 새로운 수록사항을 도입할 필요도 있다. 먼저, 용모변경자 신원확인의 어려움과 주기적으로 일제경신하는 부담을 해소하기 위해 유효기간을 도입한다. 또한, 최근 계속되는 주민등록번호 유출에 대한 대책으로서, 증 발행번호를 식별번호로 도입하여 주민등록번호를 대체한다(행정안전부, 2011f; 2011g). 온라인에서 주민등록번호 대신 아이핀(I-PIN) 사용을 권장 내지 의무화하려는 정부의 방침과 유사하게, 오프라인에서는 증 발행번호로써 주민등록번호를 대체하자는 것이다. 증 발행번호는 개인의 특성을 파악하거나 유추할 수 없도록 생성하고 본인이 원할 경우 변경할 수 있도록 운영한다는 점에서 주민등록번호와 다르다.

둘째, 민감한 개인정보 노출을 방지하기 위해 수록사항의 일부를 전자화할 필요가 있다. 현 주민등록증의 표면에 노출되어 있는 주민등록번호와 지문을 증 표면에서 삭제하고 전자 IC칩에만 수록하여 보호할 필요가 있다는 것이다. 이때 주민등록번호와 지문을

수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

11) 그런 의미에서 지난 9월 30일 발효한 제정 개인정보보호법이 “정보주체의 동의를 받은 경우”(제15조 제1항 제1호), “법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우”(동항 제2호)나 “공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우”(동항 제3호) 등에 한하여 개인정보를 수집하고 그 수집 목적의 범위에서 이용할 수 있도록 명시한 것은 이 법 제정으로 폐지된 (구)공공기관의 개인정보보호에 관한 법률에서 “공공기관은 소관업무를 수행하기 위하여 필요한 범위안에서 개인정보파일을 보유할 수 있다.”(동법 제5조)고 포괄적으로 규정하였던 것에서 진일보 한 것이라 평가할 수 있다. 이 조항은 현재의 결정에서 경찰청장이 지문 정보를 보관하는 행위의 법적 근거로 간주된 이래로, 경찰과 정부의 정보시스템이 별도의 법적 근거 없이 구축될 수 있는 포괄적인 근거로 사용되어 왔었다.

열람할 필요가 있는 경우 비밀번호 입력 또는 지문 인식을 하는 방식을 통해서 열람에 대한 본인 동의를 득할 예정이다(행정안전부, 2010c).

셋째, 주민등록증 위·변조를 방지하기 위해서 위·변조에 취약한 기존의 플라스틱 주민등록증을 대체한 전자주민증의 도입이 필요하다. IC칩에는 주민등록번호, 지문, 성명, 사진, 주소, 생년월일, 발행번호가 수록된다. 전자주민증이 도입되면, 현장에서 증 표면 내용과 IC칩 내부 정보의 일치 여부를 판독기를 통해 확인할 수 있고 위·변조 판별도 가능하다. 이를 위해 정부는 금융기관, 병원, 통신사대리점, 법무사, 중개사 등에 판독기를 총 30만 개 보급할 예정이다.

<표 1> 전자주민증 이용례

유형	이용 목적	이용 주체	이용 방식
일상 생활에서 신분확인	술, 담배, 잡지 등 성인물품 판매 연령 확인	편의점, 마트, 서점 등	주민등록증 표면 정보 확인 (플라스틱 증과 동일)
	선박료, 항공료, 관광료 할인 등 지역민 우대	선박, 항공사, 여행사 등	
	연령확인이 필요한 영화, 연극 공연 출입 등	극장, 공연장 등	
	신용카드 신청, 보험상품가입 등	카드사, 보험사, 은행 등	
주요 거래에서 신분확인	대출·담보, 부동산거래·공증, 휴대폰 개설 및 병원 진료카드 작성 등	금융기관, 병원, 통신사대리점, 법무사, 중개사	IC칩 내용 확인 및 주민등록번호 열람 (판독기 이용)
	여권발급, 운전면허증 발급 등 각종 자격증 발급	행정기관 또는 자격증 발급업체	
	출입국 관리, 선거인명부·납세자 확인, 실업급여지급 등 행정업무 수행	행정기관	
	주민등록등초본, 인감증명 등 각종 민원서류 발급 등 민원처리	행정기관	

* 출처: 행정안전부(2011c; 2011e)를 수정

부수적으로는, 전자적 방식이 아닌 탓에 무인민원발급기에서도 인식오류가 발생하고 있으며, 해외의 전자주민증 도입이 크게 증가하는 추세라는 사실도¹²⁾ 전자주민증 도입의 필요성으로 제시되고 있다.

2. 현재 심사 중인 전자주민증 관련 법안의 내용

정부가 발의한 주민등록법 개정안의 내용 가운데 전자주민증에 대한 구체적인 규정은 다음과 같다. 첫째, 주민등록증 수록사항을 추가한다. 구체적으로는 기존의 주민등록증 수록항목에 성별, 생년월일, 발행번호, 유효기간 및 ‘혈액형 등 대통령령으로 정하는 사항 중 주민의 수록신청이 있는 것’을 추가한다(개정안 제24조 제2항 제2호 내지 제3호, 제9호 내지 제10호 및 제12호). 둘째, 주민등록증에 수록되거나 표시되는 정보는 전자적으로 수록할 수 있도록 한다. 이 경우 전자적 수록의 방법, 전자적으로 수록된 정보

12) 행정안전부는 OECD 34개국 중 11개국(32%)이 전자신분증을 운영 중이고 6개국이 도입 계획이며, 전 세계적으로 43개국이 전자신분증을 시행하고 있다고 밝혔다(국회 행정안전위원회 수석전문위원, 2010; 행정안전부, 2011c).

의 타인에 대한 제공 또는 열람 방법, 보안조치 등에 관하여 필요한 사항은 대통령령으로 정한다(동조 제4항).

그러나 이에 대하여 인권시민단체의 비판이 제기되었다. 우선, ‘주민의 신청’이라는 요건과 ‘대통령령이 정하는 사항’이라는 요건을 통해 주민등록증에 수록되는 사항을 사실상 모든 개인정보로 확장할 수 있는 가능성이 있다는 우려가 제기되었고, 판독 과정에서 개인정보의 유출 위험이 지적되었다(다산인권센터 외, 2010). 의료계는 전자주민증에 혈액형 정보를 수록하는 것은 실제 수혈에서는 사용될 수 없을 뿐만 아니라 오히려 위험하다고 반대하였다(인도주의실천의사협의회, 2011; 건강권실현을위한보건의료단체연합, 2011).

그러자 행정안전부는 2011년 3월 국회 상임위원회에 수정안을 회람하며 이러한 문제를 보완하였다고 주장하였다. 주민등록증 수록항목에서 ‘혈액형 등 대통령령으로 정하는 사항 중 주민의 수록신청이 있는 것’(개정안 제24조 제2항 제11호)을 삭제하고 “혈액형. 다만, 대통령령으로 정하는 바에 따라 주민의 수록신청이 있는 경우에 한한다.”고 보다 명확히 규정하였다(수정안 제24조 제2항 제12호). 또한 새로 도입되는 주민등록증 발행번호는 개인의 특성을 파악하거나 유추할 수 없는 형태로 부여하도록 하였다(동조 제3항). 한편 주민등록증 정보의 전자적 수록에 대해서는 근거 조항을 따로 두고(수정안 제24조의2), 주민등록증에 수록되거나 표시되는 정보는 ‘주민등록증의 위조 및 변조를 방지하고 개인정보를 보호하기 위’한 목적 하에서 전자적으로 수록하도록 하고(동조 제1항) 행정안전부가 전자적으로 수록하는 주민등록증을 제작하여 보급하는 경우에 개인정보 보호에 미치는 영향과 기술적 안정성을 사전에 평가하도록 하며(동조 제2항), 전자적으로 수록된 정보를 판독기를 통하여 열람하는 경우에는 사전에 본인의 동의를 얻도록 하였다(동조 제3항). 또한 주민등록증에 전자적으로 수록된 정보는 판독기를 통하여 수집·저장할 수 없고 이를 위반할 경우 3년 이하의 징역 또는 2천만 원 이하의 벌금에 처하도록 하였으며(동조 제4항 및 제37조 제11호) 그 이외에 전자적 수록의 방법, 열람방법, 보안조치 등에 관하여 필요한 세부사항을 대통령령으로 정하도록 하였다(수정안 제24조의2 제5항).

그러나 정부의 이러한 수정안에도 불구하고, 전자주민증의 여러 가지 문제점이 여전히 해결되지 않은 채 남아 있다.

IV. 전자주민증 쟁점 사항의 검토

1. 도입의 필요성 평가

전자주민증이 기본권 침해의 과잉금지의 원칙을 위배하지 않으려면 그 도입 필요성에 드러나 있는 목적이 정당한지, 수단이 적합한지, 침해가 최소한에 그치는지, 법익의 균형을 보장하고 있는지 검토해 보아야 한다.

첫째, 신분증 수록사항의 변화나 새로운 요소를 도입하려는 목적으로 전자주민증을 도

입할 필요가 없다. 새 사진과 새 주소의 반영 및 유효기간과 증 발행번호 등 새로운 요소의 적용을 위해서 주민등록증 경신이 필요하다는 점을 인정하더라도, 그 사실이 전자적 기능을 요하지는 않는다. 수록사항의 변동은 플라스틱 주민증에도 적용할 수 있는 요소이기 때문이다. 이러한 이유뿐이라면, 굳이 IC칩을 채택할 이유도 없고 주민등록번호와 지문 등을 전자화할 필요도 없다. 그냥 현행 주민등록증의 경신주기마다 사진, 주소, 유효기간, 증 발행번호를 새로 수록해 가면 충분하다(오길영, 2011; 민주주의법학연구회, 2011).

증 발행번호가 주민등록번호를 대체하는 수단이라는 주장도 의구심을 낳는다. 행정안전부는 증 발행번호를 도입하면서 주민등록번호를 사용하지 않겠다는 것이 아니라 증 발행번호를 주민등록번호와 병행 사용하겠다는 계획이다¹³⁾. 다만 주민등록번호를 육안으로 보이지 않게 칩에 내장하여 판독기를 통해 전자적으로 열람토록 하겠다는 것이다. 비밀번호 입력이나 지문 인식의 방법으로 정보주체의 승인을 얻으면 최소한으로 이용될 것이라고 언급하고도 있다. 그러나 현재처럼 주요 거래는 물론 일상생활에서 주민등록번호에 의존하는 식별 구조가 존재하는 상황 하에서, 증 발행번호를 주민등록번호와 병행하여 사용하면 주민등록번호 위주의 식별 관행이 존속될 수밖에 없다. 따라서 증 발행번호에 주민등록번호를 대체하는 효과를 기대하기는 매우 어렵다.

둘째, 주민등록번호와 지문 등 민감한 개인정보 노출을 방지하기 위한다는 이유로 전자적으로 수록하는 것은 오히려 유출 위험을 높일 것이다. 현재까지 주민등록번호가 유출되는 경로로 주민등록증이 지적되는 경우는 거의 없다¹⁴⁾. 그러나 주민등록증에서 개인정보를 전자적으로 처리하기 시작하면 이로 인한 유출 위험이 커질 것이다. 개인정보의 유출에 따른 피해는 외관상의 노출에서뿐만 아니라, 무형적인 정보 처리의 과정에서도 발생할 수 있기 때문이다. 오히려 개인정보 침해의 양상은 첨단 정보통신망을 통한 정보의 저장, 전송, 공동이용 등에 의해 더 심각하게 나타날 수 있다. 따라서 주민등록번호와 지문을 IC칩에 내장시킨다고 해서 반드시 개인정보의 침해를 감소시킨다고 단언할 수는 없다(권건보, 2010).

전자주민증은 주민등록번호와 지문을 칩에 내장하여 육안으로 보이지 않게 할 뿐 사용하지 않겠다는 계획은 아니다. 앞서 <표 1>에서 보았듯이 정부는 편의점 등 일상생활에서 신분을 확인할 때 플라스틱 증과 동일하게 주민등록증 표면정보 확인으로 그칠 것이므로 전자적 이용이 제한될 것이라고 관측한다. 그러나 이러한 정부 주장에는 아무런 근거가 없다. 전자주민증의 민간의 이용을 명시적으로 규제하지 않는 다음에야 주민등록번호와 지문에 대한 전자적 판독이 오히려 늘어날 가능성이 크다. 특히 공공과 민간 기관에서 생체정보를 널리 사용하는 상황이 초래되는 것은 중대한 위협이다. 정부가 추진하는 본인 인증 방식은 비밀번호와 지문 인식인데, 암기를 해야 하는 전자에 비하

13) “초기에는 증 발행번호와 주민등록번호를 병행 사용하되, 일정 유효기간을 두어 주민등록번호 사용을 원칙적으로 제한(필요시 승인을 얻어 최소한으로 사용)하는 방안을 검토하고 있음”(행정안전부, 2011f).

14) “한국정보보호진흥원(KISA)에 따르면 개인정보 유출로 인한 신고와 상담 건수는 2004년 1만7569건에서 지난해 5만4832건으로 6년 새 3.1배 급증했다.”(뉴시스, 2011) 주민등록번호 등 개인정보 도용이 늘어가는 것은 옥션 등 최근 몇 년 새 인터넷으로 인한 개인정보 유출이 주요 원인으로 지적되고 있다.

여 간편한 후자가 널리 사용될 것은 자명한 이치이다. 만약 이 민감한 정보들이 장차 네트워크를 통해 유통된다면 개인정보 침해의 위험성은 더욱 증가할 것이다.

필요한 것은 전자화가 아니라 해당정보의 이용 제한과 삭제이다. 주민등록번호가 갖는 문제점은 위·변조 식별 보안장치가 내장된 IC칩에 암호화해 저장한다고 해서 근본적으로 해결될 수 있는 것이 아니다. 주민등록번호가 가진 체계상의 문제나 오남용의 문제를 방치한 채 주민등록증에 내장된 IC칩으로 숨기기만 할 경우 오히려 개인정보의 침해 가능성이 증대될 위험이 있다. 국가가 생체 인식을 사실상 조장하는 방식으로 국가신분증을 운용하는 것도 중대한 기본권 침해이다. 따라서 주민등록번호와 지문을 현행의 방식으로 수록해야 하는지 근본적인 재검토가 필요하다(권건보, 2010; 2011). 전자주민증에 통합신분증이나 전송 기능이 전혀 없다는 정부 계획대로라면, IC칩은 주민등록번호와 지문을 ‘숨기기’ 위한 장소에 불과하다. 주민등록증 수록사항에서 주민등록번호와 지문이 삭제된다면 이의 보관을 위한 IC칩 역시 불필요하다.

셋째, 전자주민증 도입의 가장 강력한 목적은 플라스틱 증의 위·변조 범죄에 대응한다는 것이다. 그런데 주민등록증 위·변조 범죄의 실제 발생 현황을 보면 이 목적의 정당성을 인정하기 어렵다. 경찰청에 따르면 위·변조 범죄 발생현황은 2007년 387건, 2008년 428건, 2009년 499건에 불과하다. 그나마 변조 범죄는 주로 청소년층에서 자신의 주민등록증 정보를 변조하는 것이다(국회 행정안전위원회 수석전문위원, 2010). 성년이 되면 해소될 청소년의 변조 행위를 이유로 전 국민의 기본권 제한이 심각할 전자주민증을 도입하는 것은 타당하지 않다. 또 다른 주요 위·변조 유형과 수법은 아예 중국으로부터 위조 주민등록증 반제품이나 완제품을 들여오는 ‘조직연계형 범죄’인데(행정안전부, 2010b) 위조 과정에는 다른 경로로부터 부당하게 획득한 개인정보가 활용된다고 한다(국회 행정안전위원회 수석전문위원, 2010). 전자주민증이 널리 유통되면 위조에 대한 수요가 늘어나고 현재처럼 조직연계형 범죄에 연루될 가능성이 커질 것이기 때문에 전자주민증의 안전성 역시 장담할 수 없다. 대다수 국민들의 주민등록번호가 유출된 상황에서¹⁵⁾ 부당하게 획득한 개인정보가 주민등록증 위조에 활용되지 않도록 완벽하게 차단할 수 있는 방법 역시 없다. 즉, 위·변조 문제에 관한 한 전자주민증 역시 완벽할 수 없고, 주민등록증 위·변조에 대한 문제 해결은 우리 사회의 주민등록번호와 주민등록증 의존성을 근본적으로 줄이는 가운데 찾아질 수 있다. 불필요하게 주민등록번호와 주민등록증을 요구하고 이에 손쉽게 의존하는 일이 줄어야 주민등록번호와 주민등록증에 대한 위·변조 수요 역시 줄 것이기 때문이다. 불행히도 행정안전부는 근본적인 대안에 관심이 없다.

2. 안전성 평가

전자주민증이 위·변조 문제에 대응하기에 적합한 수단이 아니라면 도입의 필요성이

15) 2008년 옥션에서 1천 8백만 건의 개인정보가 유출된 데 이어 2011년 7월에는 (주)SK커뮤니케이션즈에서 운영하는 네이트와 싸이월드에서 3천 5백만 건에 달하는 개인정보가 유출되었다.

줄어들 수밖에 없다. 이러한 우려에 대하여 행정안전부는 전자주민증의 IC칩을 열람하는 과정에서 개인정보 유출의 위험이 발생하지 않도록 기술적, 제도적, 관리적 보안대책을 수립하여 추진할 예정이라고 밝혔다(국회 행정안전위원회 수석전문위원, 2010; 행정안전부, 2011c; 2011e). 먼저 기술적 보안대책으로서 국제공통평가기준(ISO/IEC CC 인증)에 따라 보안성이 검증된 IC칩을 적용하고, 판독기는 화면을 통해 개인정보를 육안으로만 확인하고 수집·저장·유출되지 않도록 구현할 것이라고 한다. 정부는 불법적인 판독기가 등장할 수 없도록 판독기 소프트웨어의 주기적 업그레이드 등 판독 소프트웨어 관리를 위한 보안대책을 충분히 검토하여 시행할 예정이라고도 한다. 제도적 보안대책으로서는 판독기를 통한 전자적 수록정보의 수집·저장 금지를 법률에 명시하고, 이를 위반할 경우 벌칙을 적용하겠다고 한다. 관리적 보안대책으로서는 개인정보영향평가 및 기술적 보안성 평가를 사전 시행하여 개인정보 침해 위험요인을 차단하겠다고 한다.

하지만 기술적 대책에 있어 IC칩이 다음 유효기간까지 안전할 것이라고 기대할 수 없다¹⁶⁾. 기술발달 속도에 비추어볼 때 현재의 안전한 기술이 미래에도 계속 안전한 것이라는 장담은 누구도 할 수 없기 때문이다¹⁷⁾. 우선 판독기의 불법 개조나 해킹이 가능하다. 판독기를 통한 개인정보 유출은 대규모로 이루어질 수 있다는 점에서 특히 위험하다. 비접촉식 IC칩은 그 특성상 3~10cm 이내 거리에서 무단으로 열람될 위험성을 내포하고 있음은 행정안전부가 인정하는바 대로이며¹⁸⁾, 판독기 업그레이드를 위한 입출력 장치를 통하여 정보가 유출될 수도 있다. 행정안전부는 이의 방지책으로서 주민증을 제시받은 업무처리자가 발행번호를 입력하도록 하고 민원인이 비밀번호를 입력하도록 한다는 안을 제시하고 있지만(행정안전부, 2011a), 이는 발행번호와 비밀번호가 함께 수집되거나 유출되면 다른 정보 유출도 가능하다는 의미이기도 하다. IC칩 자체가 해킹되는 경우에는 전 국민의 전자주민증을 전량 교체해야 할 위험에 처할 수 있다¹⁹⁾. 이는 행정안전부가 주장하는 대로 판독기의 소프트웨어를 업그레이드함²⁰⁾으로써 해결될 수 있는 문제가 아니기 때문이다.

전자주민증의 잠재적인 위험 요소는 비전자 신분증의 위험요소에 비교할 수 없을 정도로 크다. 과거 한국전산원은 비전자 신분증의 위험요소가 ‘증’ 자체의 위·변조에 집중되어 있는데 비해, 전자 신분증의 위험요소는 발급부터 이용까지 전자적으로 처리되는 전 과정에 존재한다는 점을 지적한 바 있다(한국전산원, 1996). 즉, 발급센터 시설물에

16) 2008년 국정감사에서 진수희 의원은 금융 IC칩의 복제가 가능하다는 사실을 밝혔으며(뉴시스, 2008), 송영선 의원은 국감장에서 전자여권의 무선 해킹 시연을 해보이기도 하였다(뉴스라이브, 2008).

17) “현행 주민등록증 역시 도입당시에는 위·변조를 방지하기 위한 장치가 마련되어 있다는 평가를 받았으나, 이후 기술의 발전으로 인해 위·변조가 쉽게 되어 버린 것은 이러한 측면의 사례로 언급될 수 있을 것이다.”(김주영, 2011)

18) “IC칩의 특성상 3~10Cm 이내 리더기에서 정보가 읽힐 수 있는 위험”(행정안전부, 2011a).

19) “먼저 IC칩 자체가 해킹된 경우, 이를 판독기의 업그레이드를 통해 치료한다는 것은 그 발상부터 이상한 이야기이다. IC칩 자체가 해킹되었다면, 당해 IC칩이 장착된 카드를 폐기해야 하는 것은 너무나 당연한 것이다 … 금융감독원의 IC 카드 사건에서도, 업그레이드가 아니라 전량 ‘교체’하기로 했음은 이러한 점을 잘 보여주는 사례이라 하겠다.”(오길영, 2011; 민주주의법학연구회, 2011)

20) “해킹기술 발전에 대비, 불법개조 및 해킹 여부 등을 모니터링하고 전용SW를 주기적으로 업그레이드”(행정안전부, 2011c).

대한 위법한 접근, 발급센터의 전산망 시스템에 대한 침해, 발급센터 시설물과 전산망에 대한 자연재해(수해, 화재, 정전, 지진 등), 발급센터와 관련기관 운영자에 의한 대규모 정보유출, 발급센터에 LAN(근거리통신망), WAN(원거리통신망)으로 연결되어 있는 관련 통신망과 온라인무인발급기를 통한 침해, 카드 외부기재사항 위·변조, IC칩 내용의 전부 복제, IC칩 내용의 위·변조, 백지카드의 부정유출, 카드 자체의 부정발급, 분실카드의 무단사용, IC칩 기재사항의 불법열람 등 전자 신분증은 다양한 내외부 정보처리 과정에서 유출 위험성을 가지고 있다. 특히 공공기관의 개인정보 오남용과 유출 사고에 있어서 해킹 등 외부자에 의한 요인 뿐 아니라 내부자에 의한 요인이 상당히 많다는 사실에 주목할 필요가 있다²¹⁾. 실제로 전자여권의 경우 발급업체를 통해 국무총리, 장관할 것 없이 92만여 명의 개인정보가 유출되기도 하였다(김호연, 2011).

유럽 네트워크 및 정보보호진흥원(ENISA·Europe Network & Information Security Agency) 역시 전자주민증의 취약점으로 다음과 같은 사항을 제시하고 있다(ENISA, 2009). 첫째, 전자주민증 설계상의 결함으로서, 해커(attacker)나 이용자의 보안키 취득 허용, 해커의 전자주민증 복제 허용, 해커나 이용자의 전자주민증 정보 변조 허용, 해커가 훔친 카드나 위임된(delegated) 카드에서 비밀번호 획득 허용이 발생하는 경우. 둘째, 암호화나 인증 프로토콜, 또는 실행상의 취약성으로서, 암호키가 너무 짧거나 예측가능한 비밀번호, 깨어진 암호 알고리즘, 재전송 공격(replay attack)을 허용하거나 추가적인 보안을 제공하지 않는 프로토콜, 이러한 프로토콜 실행상의 취약성이 존재하는 경우. 셋째, 단말기의 취약성으로서, 트로이 목마, 불법적인 브라우저 플러그인 다운로드, 불법적인 SSL 인증을 허용하는 소프트웨어나 실행과정상의 취약성이 존재하는 경우. 넷째, 특정한 공격을 허용하는 인증 아키텍처와 프로토콜의 취약성으로서, 상호 인증의 부족, 인증 과정에서 물리적인 토큰 불요구, 크리덴셜의 기한 미종료, 대역외부(Out-of-Band) 인증의 부족, 요구되는 것보다 더 많은 개인정보의 거래 인증이 발생하거나, 비밀번호나 크리덴셜이 너무 짧을 경우. 다섯째, 기반시설의 취약성으로서, DNS 스푸핑이나 포이즈닝, DDOS 공격 등이 가능한 경우. 여섯째, 이용자의 행위나 인지 부족 문제로서, 피싱 메일, 불법적인 인증, 세션 미종료, 전자주민증 임대 등이 발생하는 경우. 일곱째, 전자주민증 절도가 발생하는 경우이다. 이런 위협을 행하는 행위자에는 악의적인 해커도 있지만, 서비스 제공자도 주요 행위자 중 하나이다. ENISA는 “개인정보는 상업적 목적으로 수집되고 사용되며 심지어 판매될 수 있다”는 점을 경고하고 있다. 한국에서도 개인정보 유출의 주요 요인 중 하나는 개인정보 취득으로 인한 경제적 이득이라는 점을 비추어볼 때 이는 우리에게도 유효한 경고이다.

이러한 여러 가지 위협 요인 때문에 다른 나라의 경우에는 전자주민증을 도입하더라도 무조건적인 안전을 장담하기 보다는 ‘정보분리의 원칙’²²⁾ 하에 시스템을 분산시키거

21) 감사원은 공무원이 주민등록정보 등 개인정보를 사적으로 무단 열람하고, 외부로 유출하는 문제를 완전히 차단하긴 어렵다고 보았다(감사원, 2008). 2006~2009년에는 총 343명의 공공기관 직원이 개인정보 유출로 징계를 받았고(동아일보, 2011), 2010년 공공기관의 개인정보유출사고는 모두 1천196건으로 이 가운데 업무 담당자의 부주의로 인한 사고가 558건(46%)을 차지하였다(연합뉴스, 2011).

22) “특정된 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 원칙적으로 통

나 ‘선택권’을 존중하는 예방적 접근을 취하고 있다. 예컨대 독일은 개인번호나 지문을 국가 중앙 차원에서 관리하지 않으며, 전자 기능의 삽입과 지문 수록을 선택 사항으로 인정하고 있다. 실제로 독일에서는 전자주민증 도입 이후에도 전자 기능을 배제하는 경우가 많이 발생하고 있는데, 이는 전자신원증명의 보안성과 안전성에 대한 우려 때문이다(이재경, 2011). 스웨덴, 핀란드, 일본 등에서도 본인의 신청이 있을 때만 전자신분증을 발급해주고 있을 뿐이다(권건보, 2011).

그런데 이들 국가와는 달리 한국에서는 전 국민을 대상으로 하는 의무적인 주민등록번호제도와 지문날인제도를 시행하고 있어서 전자신분증의 도입에 따른 폐해가 훨씬 심각하다고 볼 수 있다(권건보, 2011). 국가는 출생 시점부터 전 국민에게 주민등록번호를 부여한 후 이 번호를 기준으로 한 주민등록을 국가 차원의 중앙 데이터베이스에서 관리하고 있으며, 행정정보공유시스템을 통해 이 정보를 은행과 같은 민간 기관을 포함한 53개 기관과 온라인으로 상시 공유하고 있다(행정정보공유추진위원회, 2011). 국민은 국가신분증 발급에 응해야 하며 주민등록증 발급 시 지문의 날인과 그 수록도 강제 사항이다. 따라서 이미 전자주민증을 도입한 다른 나라들과 비교하여 보아도 한국에서 전자주민증을 도입할 때의 위험성이 무척 높을 수밖에 없다.

그런데도 우리 정부의 개정안이나 수정안은 제도적 대책으로 전자적인 수록정보를 판독기를 통하여 수집·저장할 수 없다는 규정을 두고 있을 뿐, 다른 방법으로 전자 정보가 유출되는 경우에 대해서는 전혀 규제하지 않고 있다. 정부의 방침과 다른 판독기의 하드웨어나 소프트웨어가 시중에 유통될 가능성도 있다. 개인정보를 요구하는 국내외적 사회경제적 동기가 법문상의 처벌규정을 압도할 가능성이 매우 크다.

따라서 그 구체적인 사양도 공개되지 않았고 검증도 되지 않은 기술적 안전성에 대하여, 정부의 장담을 막연하게 믿고 국회가 전자주민증을 심사해서는 안 될 것이다. 행정안전부가 관리적 대책으로 추진하겠다는 기술적 안정성과 개인정보영향에 대한 평가는 자부처에서 시행하는 것이기 때문에 객관적인 평가를 기대하기 어렵다.

그 외에도 주민등록증 수록사항을 판독기를 통하여 수집·저장할 수 없도록 하겠다는 법규안에는 현실적인 한계도 있다. 정부가 행정기관은 물론 금융기관, 병원, 통신사대리점, 법무사, 중개사 등에 판독기를 널리 보급할 예정인 만큼, 공공기관과 민간 기관에서의 전자주민증의 사용 목적이 현재의 주민등록증 사용 목적과 크게 달라지지 않을 것이다. 그런데 정부의 계획대로라면 전자주민증에서 주민등록번호는 IC칩에만 수록되어 있고 이에 대한 수집과 저장이 기술적으로 불가능하다. 즉, 주민등록번호에 대한 열람만 가능하고 사본 생성이 불가능하다는 말이다. 그렇다면 정부는 공공과 민간 기관에서 주민등록번호 혹은 주민등록번호가 포함된 신분증 사본을 보관할 필요가 있는 업무를 앞

합되지 않고 분리된 상태로 유지되어야 한다. 따라서 어떤 기관이 보유하고 있는 개인정보를 데이터베이스를 구축·통합하거나 다른 기관에 제공한다면 자동검색시스템을 통해 개인정보를 공동으로 활용한다면 하는 것은 원칙적으로 금지된다. 이러한 내용은 독일 연방헌법재판소가 인구조사판결에서 언급한 ‘정보상의 권력분립’의 원칙과 같은 것이라 할 수 있을 것이다. 국가권력이 정보통일체로서 단일화되는 것은 용납되지 않는다는 동 재판소의 선언은 국가행정조직이 다른 목적으로 개인정보를 이용할 소지가 있는 개별 행정부서들에 의한 정보 접근이 차단되도록 구성되어야 할 것을 요청하는 의미를 가지는 것으로 이해되고 있다.”(권건보, 2005: 222면)

으로 어떻게 처리하도록 할 계획일까? 물론 이번 기회에 공공과 민간 부문에서 주민등록번호의 사용과 보관이 단번에 일소된다면 무척 혁신적일 것이다. 이를 위해서는 금융 실명거래 및 비밀보장에 관한 법률을 비롯하여 신원 확인에 대한 규정을 가지고 있는 법률들을 모두 개정해야 할 것이다(김민호 외, 2009). 하지만 우리 정부에는 그럴 의지가 사실상 전혀 보이지 않으니 해당 조항의 실효성을 의심할 수밖에 없다.

3. 침해의 확장 가능성 평가

앞서 살펴보았듯이 전자주민증의 도입 필요성이나 위·변조로부터 안전성이 뚜렷하지 않은 상황이다. 그런데도 정부는 15년 간 명분과 사양을 바꾸어 가며 국가신분증의 전자화에 집착해온 것이 사실이다. 따라서 전자주민증에 대한 중대한 우려 사항은, 전자기능의 효율성을 최대화하려는 의도가 숨어 있을지 모른다는 것이다. 전자주민증의 기능이 도입 당시 심사되었던 사양 이상으로 확장되면 그 침해성이 커질 것은 자명하다. 대표적인 의혹이 통합신분증의 등장과 네트워크 연동이다. 정부는 전자주민증에 통합신분증이나 전송 기능이 전혀 없다는 사실을 계속하여 강조하여 왔다²³⁾. 그러나 IC칩에는 기술적인 확장성이 존재하는 반면, 개정안과 수정안 어느 곳에도 이러한 기능의 확장을 방지할 수 있는 법규정이 부재하다.

첫째, 통합신분증으로의 확장 가능성이 있다. 잘 알려진 대로 1990년대 전자주민카드 계획은 한 장의 카드에 주민등록증, 주민등록등본, 초본, 운전면허증, 의료보험증, 국민연금증서, 인감 등 7개 분야 47개 정보를 수록한 통합카드로 계획되었다. 2006~2007년 도입이 추진되었던 차세대 주민등록증 발전모델 연구결과에서도 연계키 수록을 통해 운전면허·건강보험 등 다른 신분증과의 연계방안이 검토된 바 있다. 따라서 현재 추진되는 전자주민증 역시 통합신분증으로 발전할 가능성에 대한 의구심이 줄지 않고 있다. 하나의 카드를 다목적으로 사용하는 통합신분증은, 서로 다른 목적으로 수집되고 집적된 개인정보를 연계 내지 통합하여 개인정보의 최소 수집의 원칙 및 목적 외 이용 금지를 사실상 형해화하고 개인정보 자기결정권을 중대하게 침해한다. 안전성에 있어서도 취약하다(ENISA, 2009). 이에 대하여 행정안전부는 주민등록법에 명확한 규정 없이 다른 법률에 근거하여 주민등록증과 다른 신분증을 연계·통합할 수 있다는 우려는 사실과 다르다고 해명하였다. 운전면허, 건강보험 등 다른 신분증과의 정보 연계를 위해서는 IC칩에 연계키를 수록하여야 하며, 이는 주민등록증 수록항목으로서 주민등록법 개정이 필요한 사항이라는 것이다(행정안전부, 2011e). 그러나 개정안과 수정안 어디에서도 전

23) “이번에 추진하는 전자주민등록증에는 공인인증서, 운전면허증, 건강보험증 등의 다른 정보를 기재하지 않으며, 통합신분증 역할을 하는 방안도 전혀 검토하지 않고 있습니다.” ; “전자주민등록증은 필요 시 주민등록증에 수록된 내용을 리더기[판독기를 의미함 - 옮긴이]로 확인만 할 뿐 주민등록증 정보가 수집·저장되거나 다른 어떤 데이터베이스와 연계하여 기록을 남기는 것이 아니므로 감시사회가 될 것이라는 우려는 전혀 근거가 없습니다.” ; “주민등록증은 개인 신상기록카드가 아니므로 장애인 여부나 개인건강기록을 넣을 필요성도 없으며, 그러한 계획도 전혀 없습니다.”(행정안전부, 2010a); “전송망을 통해 중앙데이터베이스의 정보를 읽는 방식이 아님”(행정안전부, 2011c).

주민증에 대한 ‘정의규정’을 따로 두고 있지 않은 상황에서, 비밀번호, 암호키 등 ‘기술적 세부사항’에 대하여서는 법에 명시된 주민등록증 수록사항과 별도로 시행령으로 규정하도록 되어 있다(수정안 제24조의2 제5항). 그렇다면 건강보험 등 특정한 신분 데이터베이스에 인증할 수 있는 ‘연계키’가 ‘기술적 세부사항’으로서 추후 삽입될 가능성을 법률적으로는 전혀 배제할 수 없는 것이다²⁴⁾. 주민등록번호나 지문 그 자체가 타 데이터베이스 연계를 위한 연계키로 사용되어 사실상 신분증 통합이 이루어질 가능성도 배제할 수 없다.

둘째, 개인정보의 네트워크 전송과 집적의 가능성이 있다. 실제 영국 등 해외 개인정보보호 감독관의 주요 우려 사항 중 하나가 전자주민증 이용기록이 디지털 족적으로 남는 것이다(Information Commissioner's Office, 2005). 전자주민증이 국가 신분 시스템에 확인될 때마다 데이터 역사(trail)가 생성되면 추후 이에 대한 열람과 제공 등을 통해 한 개인에 대한 총체적인 감시와 추적이 가능하기 때문이다. 정부는 전자주민증의 위·변조 확인은 증의 표면정보와 IC칩 정보를 비교하는 방식이기 때문에, 온라인 대조가 필요 없다고 말한다²⁵⁾. 그러나 이는 주장일 뿐, 개정안과 수정안 어디에도 개인정보의 온라인 전송을 금지하는 규정을 찾아볼 수 없다. 수정안 제24조의2 제4항에서 주민등록증에 전자적으로 수록된 정보는 판독기를 통하여 수집·저장할 수 없도록 한 규정은 판독기 내부에 대한 수집·저장을 금지하는 것으로 국한된다²⁶⁾. 판독기를 네트워크에 연결할 경우, 수정안대로 판독기로 정보를 수집, 저장한 경우의 처벌 규정만으로 정보 수집이나 저장행위를 예방하기 어렵다(참여연대, 2011).

또한 주민등록증 진위 확인을 이유로 추후 온라인 연계에 대한 수요가 상당히 발생할 것으로 예측된다. 현재도 ARS(전화 1382), 민원24 창구를 통해 주민등록증의 진위에

24) “나아가 수정안이 입법에 있어 가장 기본이 되는 ‘정의규정’조차 마련하지 않은 것이, 절묘한 우연인 것인지도 묻고 싶다 … 혹시나 ‘증’에 부착되어 있는 IC칩은 법문의 표현처럼 ‘전자적 수록의 방법’에 불과하여 제외되는 것은 아닌가? 기술적인 상재를 덧붙이자면, IC칩 속에 포함되는 메모리 공간, 즉 EEPROM, RAM, ROM 가운데 어느 부분까지가 정확히 주민등록증의 일부인가 하는 점이다. 나아가 보안용 코드도 수록사항에 포함되어야 하는 것은 아닌가? 아니라면 인증용 코드는 어떠한가? 즉 기술적 필요로 인해 수록되는 정보들은 수정안의 제24조 제2항의 수록사항에 포함되지 않아도 당연한 것인가 하는 점이다. 그 어떤 이도, 현재로서는 도무지 알 방도가 없다. 이러한 입법태도는 우연이라고 하기에는 너무나 극적이라고 판단된다. 실제 행정안전부가 IC칩의 제원에 대해 전혀 아는 바가 없거나, 그렇지 않다면 이렇듯 적당히 얼버무리므로써 무언가를 의도하고 있는 것이다. 만약 준비성이 많은 누군가가 차세대 전자주민증을 대비하여, 형사사법 정보시스템에서 전과기록과 연계할 수 있는 Key값을 전자주민증의 정의규정에 포함되지 않는 메모리에 슬쩍 넣어두거나, 기술적 필요로 인해 수록되는 각종의 정보 속에 포함시켜 놓는다면 어떻게 할까? 현재의 주민등록법 체제에서는 이에 대해 법적으로 대응할 수 있는 방법은 전혀 없다.”(오길영, 2011; 민주주의법학연구회, 2011).

25) “전자주민증의 위·변조 확인은 증의 표면정보와 IC칩 정보를 비교하는 방식이기 때문에, 온라인 대조가 필요 없고 온라인화할 계획도 없음”(행정안전부, 2011d). 추후 제작성된 같은 제목의 문헌에서는 이 표현이 “전자주민증의 위·변조 확인은 증의 표면정보와 IC칩 정보를 비교하는 방식이기 때문에, 온라인 대조가 필요 없음”이라고 변경되어 ‘계획’에 대한 확인이 사라졌다(행정안전부, 2011e).

26) “수정안의 어느 조항을 살펴보아도 네트워크 케이블이 판독기에 설치되지 않는다는 언급을 찾아볼 수 없다 … ‘해킹 여부 등을 지속적으로 모니터링하고 판독기의 전용 소프트웨어를 주기적으로 업그레이드’하기 위해서는 반드시 네트워크 케이블이 장착되어야만 할 것이다.”(오길영, 2011; 민주주의법학연구회, 2011).

대하여 확인을 요청하는 수요가 일 평균 10만 건에 달한다. 공공과 민간 부문에서 주민등록증이 널리 사용되고 있으니 그에 대한 진위 확인 수요 역시 많을 수밖에 없는 것이다. 행정안전부가 제시한 증 표면과 내부 정보 비교 방식으로는 표면과 내부가 동시에 위·변조 되었을 경우나 분실증 등 타인의 주민증을 사용하는 경우를 판별해낼 수 없다. 따라서 이러한 위·변조 사례에 대응하는 가장 강력한 진위 확인 방식은 중앙 주민데이터베이스에 질의하여 실제 존재하는 주민등록증인지 여부를 확인하는 것이다. 정부는 발행번호, 발급일자, 주민등록번호를 확인하는 방식으로 이 서비스를 존속할 계획이지만²⁷⁾, 온라인 연계 가능성은 부인하고 있다. 그러나 판독기에 업그레이드를 위한 입출력 장치가 장착되어 있는 만큼, 추후 진위 확인 서비스가 온라인을 통해 실시간으로 이루어질 가능성이 분명히 있다.

장차 온라인 전송을 금지하기 위해서는, 정보통신망을 이용하거나 중앙 주민데이터베이스에 질의하여 전자주민증 수록내용의 진정성에 대하여 확인할 수 없도록 규정하거나 질의내역을 저장할 수 없도록 규정하고, 정보통신망에서 전자적 방법의 신분확인용으로 전자주민증을 사용할 수 없다는 규정이 명시되어야 마땅하지만 현재의 개정안과 수정안에는 이러한 규정을 찾아볼 수 없다.

그밖에 개정안과 수정안 모두 시행령 위임 범위가 넓다는 점은 여전한 문제이다. 일반 국민들로서는 대통령령에서 전자적 수록의 대상, 방법, 활용의 범위 등이 구체적으로 어떻게 규정할 것인지 짐작하기란 결코 쉽지 않다. 여기서 IC칩에 어떠한 정보를 내장할 것인지, 내장된 정보를 어떻게 전자적으로 확인할 것인지 등에 관한 사항은 정보주체에게 있어서 기본권의 실현을 위하여 매우 중대한 사항이다. 그럼에도 불구하고 전자적 수록에 관한 사항을 법률에서 범위의 제한도 가하지 않고 죄다 대통령령에 의해 규정하도록 위임한 것은 포괄적 위임입법 금지의 원칙에 어긋나는 것으로 평가될 소지가 크다(권건보, 2010)²⁸⁾.

또한 판독기를 통하여 알게 된 개인정보를 목적 외로 사용하거나 제3자에 대해 제공 하는 경우를 금지하거나 처벌하는 규정이 누락되어 있고, 주소 변경 등 내용 변경 및 재발급에 대한 규정도 미비하며, 주민등록증 위·변조에 대한 구체적인 처벌 규정 또한 미비하다는 점도 지적하여 둔다(송희준 외, 2007).

IV. 주민등록제도의 검토

27) “진위확인이 필요하나 리더기가 없을 경우 인터넷서비스(민원24) 및 자동응답전화를 통해 정보 확인 가능토록 서비스 제공”(행정안전부, 2011c).

28) “만일 전자적 수록의 필요성을 인정할 수 있다면, 전자적 수록의 한계를 법률에서 어느 정도 명시한 다음에 대통령령에 위임하는 것이 바람직할 것이다. 적어도 법률에서 ‘주민등록번호, 지문 기타 민감한 개인정보’를 전자적 수록의 대상으로 한다면 하는 제한의 규정을 둘 필요가 있다. 나아가 전자적 수록은 IC칩 등에 내장하는 등의 방법으로 한다면, 전자적으로 수록된 정보를 판독하는 장치에는 저장의 기능을 사용할 수 없다면, 혹은 전자적으로 수록된 정보는 원칙적으로 정보통신망을 통해 전송할 수 없다면 하는 등의 규정도 둘 필요가 있다고 본다. 아울러 법률에서 민간영역에서 리더기를 사용할 수 있는 기관을 일정한 범위로 한정하여야 할 것이다.”(권건보, 2010; 고문현 외, 2010).

1. 주민등록제도의 인권침해성

주민등록증 경신에 있어 우선적으로 고려할 사항은 전자적 기능의 도입 여부보다 인권침해적인 요소에 대한 재고이다. 대표적인 사항이 주민등록번호와 지문 수록, 그리고 주민등록증의 의무발급 문제이다.

주민등록증제도는 애초부터 복지행정 등의 대국민 행정에서 수급자의 신분확인을 보다 용이하게 하기 위한 것이 아니라, 간첩이나 불순분자를 용이하게 식별·색출하여 반공태세를 강화하기 위한 것이었다. 따라서 신분확인을 위한 최소한의 정보(이름, 사진, 주소)만을 수록한 것이 아니라, 범죄자를 쉽게 색출하기 위한 여러 정보들(지문, 병역사항, 본적, 호주, 고유일련번호 등)을 포함하여 주민등록증에 수록하게 된 것이다(김주영, 2011). 주민등록제도의 제정과 개정의 전 과정에 걸쳐 정보인권 문제가 필연적으로 불거질 수밖에 없다.

우선 주민등록증에 주민등록번호의 수록을 재고할 필요가 있다. 오늘날 한국사회에서 계속되는 주민등록번호 유출 문제는 시민들의 프라이버시를 중대하게 위협하고 있다. 주민등록번호가 연령, 성별, 지역 등 개인정보를 내포하는 조합체계를 가지고 영구적인 고유식별자로 기능하고 있으며, 공공과 민간의 영역에 걸쳐 광범한 목적에 활용되도록 요구되고 있는 것은 문제가 아닐 수 없다. 뿐만 아니라 주민등록번호가 전산망에 의해 분리된 개인정보들이 서로 비교되거나 통합될 수 있도록 연결시키는 매개체로 활용될 경우 국민은 정보의 객체로 전락할 우려가 큰 것도 사실이다. “주민의 거주관계 등 인구의 동태를 상시로 명확히 파악하는”(제1조) 것을 목적으로 하는 주민등록법상 전 국민에 주민등록번호를 부여하는 것 자체에 위헌 소지가 있다(김일환, 2005). 주민등록번호의 유출 및 오남용 위험성과 위헌성을 제고하기 위하여 주민등록증에서 주민등록번호를 삭제할 필요가 있는 것이다. 그러나 증 표면에서 주민등록번호를 없앤다고 해서 그것으로 주민등록번호에 대한 사회적 수요가 완전히 사라지는 것은 아니기 때문에, 주민등록번호를 요구할 수 있는 사용 범위를 고유의 행정 목적으로 엄격하게 제한하는 등의 입법적 조치가 필요하다²⁹⁾. 또한 주민등록번호의 조합체계를 개인식별의 가능성을 낮추는 방향으로 변경하고 주민등록번호를 대체하는 수단을 강구하는 한편으로, 법률상 주민등록번호의 고지를 의무화하고 있지 않은 분야에서 주민등록번호의 고지를 거부하더라도 불이익을 가할 수 없도록 명문화하는 조치도 필요하다(김일환, 2005; 권건보, 2010; 고문현 외, 2010).

또한 주민등록증상의 지문 정보가 불필요하다는 지적이 오래 전부터 계속되어 왔다. 실제 국가 행정사무에서 지문 정보의 활용은 주로 범죄의 수사 등에 활용되기 때문에 주민등록제도 본연의 목적과 거리가 있으며, 주민등록증에 기재된 지문 정보가 주민등

29) 캐나다 등 우리의 주민등록번호와 유사한 사회보험번호 제도를 가지고 있는 국가들도 그 용도를 벌금부과, 소득세 징수, 실업급여 등에 한하여 법률로써 제한하고 있는 경우가 많으며, 번호의 제시를 요구하는 경우 개인에게 제시요구의 목적과 강제성 여부, 제시 거부시의 결과에 대하여 미리 고지하도록 하고 있다(김일환, 2005).

록제도와 관련하여 사용되는 예도 없다. 무엇보다 주민등록 발급 시 모든 국민을 상대로 열 손가락의 지문을 강제로 날인하도록 하고 그중 일부를 주민등록증에 수록하도록 하는 것은 모든 국민을 잠재적 범죄자로 취급하여 존엄성을 위협하는 것과 같다(김일환, 2005; 김주영, 2011; 권건보, 2011). 특히 전자적 방식으로 지문 정보 활용이 늘면 생체정보가 오·남용될 소지가 높아지는 만큼 지문 정보의 주민등록증 수록은 재고해야 한다.

전반적으로 신분 확인 관행에 대한 성찰이 필요하다. 신분 확인에 대한 과도한 요구가 주민등록번호를 비롯한 개인정보의 수집과 이용을 조장하기 때문이다. 온라인에서 인터넷 실명제가 강제되면서 인터넷서비스제공자들의 개인정보 수집이 늘고 이에 대한 공격 또한 늘면서 개인정보 유출이 대규모로 발생하고 있음은 주지하고 있는바 대로이다. 따라서 온라인 개인정보 유출을 방지하는 대책은 온라인 주민등록번호 수집을 최소화하는 것이다(심우민, 2011). 오프라인 신분증에 대한 위·변조 수요를 억제하는 대책도 역시 불필요한 신원 확인 요구를 제한하는 것일 수밖에 없다.

주민등록제도의 근본적 변화 없는 전자주민증은 개인정보보호의 수단이 아닌 또 다른 개인정보를 유출할 수 있는 창구를 확대하는 것에 불과하고 불필요하게 본인인증을 더욱 확대함으로써 개인정보보호라는 시대적 요구에 역행하는 제도이다(경제정의실천시민연합, 2011). 전자주민증이 보급되면 일상생활 곳곳에서 신분 확인을 위한 신분증 판독이 늘어날 것이다. 이는 익명의 권리를 침해하는 중대한 기본권 제한임에는 물론이고³⁰⁾ 법적 근거가 없는 신분 확인 요구를 널리 확산시킬 것이다. 실제로 행정안전부는 ‘타인 명의 휴대폰 개통’의 방지하기 위한 용도로 이동통신 대리점에서 전자주민증을 활용하는 예를 제시하여 왔다(행정안전부, 2010b; 2011e). 현행 법률로 휴대전화 실명 가입이 법규 사항이 아닌데도 신분 확인이 유도되고 있는 것이다. 전자주민증에 대한 요구와 사용이 늘어갈수록 전자주민증을 기초로 한 신분증 통합 수요가 발생할 것 또한 예측할 수 있다.

정부는 주로 연령 확인 용도로 주민등록증을 사용하는 편의점, 유흥업소 등에서는 증표면정보를 확인하는 방식으로 판독기 수요를 감축해갈 수 있다고 주장하지만(행정안전부, 2011c; 2011e), 이들 업체야 말로 현재 청소년 층에서 주민등록증이 변조되어 사용되는 주요 공간이고 진위 확인 수요가 많은 곳이기도 하다. 따라서 이들 업체에서 판독기가 불필요할 것이라는 주장은 개연성이 없다.

마지막으로 국가신분증 의무발급은 기본권 제한 소지가 매우 크기 때문에 많은 나라들이 선택적 발급제도를 두고 있다는 점을 상기하고자 한다. 의무적 국가신분증 제도를 두고 있는 독일의 경우에도 전자 기능의 도입은 선택사항이라는 점에 주목해야 한다.

2. 해외 사례

30) “‘자유로운’ 표명과 전파의 자유에는 자신의 신원을 누구에게도 밝히지 아니한 채 익명 또는 가명으로 자신의 사상이나 견해를 표명하고 전파할 익명표현의 자유도 그 보호영역에 포함된다.” 헌재 2010. 2. 25, 2008헌마324, 2009헌바31 병합, 공직선거법 제82조의6 제1항 등에 대한 위헌확인 및 위헌소원 사건.

정부는 OECD 34개 국가 중 11개 국가에서 IC칩을 탑재한 전자신분증을 운영 중이며, 6개국에서 도입 추진 또는 논의 중에 있다고 주장한다(행정안전부, 2011c; 2011e)³¹⁾. 그러나 이들 국가 상당수는 한국과 상황이 매우 다르다³²⁾. 특히 유럽연합 국가들은 통합국가의 건설 과제 앞에서 전자신분증의 보급을 추진하고 있다는 특수성이 있다³³⁾. 그러나 여전히 유럽 국가 내부에서도 전자주민증에 대한 거부감이 만만치 않은 가운데³⁴⁾, 전자주민증을 도입한 국가들이라 하더라도 한국처럼 의무발급, 주민등록번호, 지문날인을 모두 한 제도 안에 포함하는 경우는 거의 찾아보기 힘들다(고문현 외, 2010).

전자주민증을 도입한 것으로 알려진 각국의 사례를 구체적으로 살펴보면 다음과 같다.

우선 독일은 2010년 11월 1일부터 전자신분증을 도입하고 전자칩에 지문, 사진, PIN 번호를 넣었으나, 전자 기능의 삽입 여부를 개인이 선택하도록 하였다. 지문 역시 개인의 선택에 따라 카드에만 저장하고 중앙 차원의 데이터베이스에 저장하지 않으며 경찰, 세관, 증 관련관공서 등 일부 기관에서만 읽을 수 있다. 전국적인 개인번호는 부여되지 않고, 신분증을 발급할 때 부여하는 일련번호는 새로운 신분증을 발급할 때 새로 부여되며, 일련번호에 인적 사항이나 기타 사항을 암시하는 내용을 담을 수 없고, 공공 부문은 물론이고 민간 부문에서도 일련번호를 자료에서 인적사항을 추출하는 것 또는 자료의 결부를 가능하게 하는데 이용할 수 없다(고문현 외, 2010).

이탈리아는 의무발급이 아니고, 기존 신분증과 전자주민증이 병행 발급된다(Whitley, 2005; 2009; Wikipedia, 2011a). 국가신분증의 지문 수록은 명시적으로 시민이 의사를 표시할 때만 이루어지도록 법령을 두고 있어 자발적으로 이루어진다. 데이터베이스는 분산형이다(Whitley, 2009; Statewatch, 2011).

31) 그러나 행정안전부는 11개국이 어디를 의미하는지를 명확히 밝히지 않았다. 이하에서는 국회 행정안전위원회 수석전문위원(2010) 검토보고서에서 OECD 국가 중 전자주민증을 도입한 것으로 표기된 12개국의 예를 검토하되 노르웨이를 제외하였다. 노르웨이는 전자주민증이 도입되지 않은 것으로 보고되고 있다(Statewatch, 2011; Wikipedia, 2011b).

32) 이하의 각국 상황에 대한 분석은 기본적으로 국회 행정안전위원회 수석전문위원(2010) 검토보고서에 따른 것이고, 검토보고서에 의하지 않은 경우에만 출처를 별도로 표시하였다.

33) 예컨대 영국 전자주민증은 2005년 12월 EU에서 “common standards for security features and secure issuing procedures for ID cards”가 발표된 이후 가속화되었다고 평가된다(COUNCIL OF THE EUROPEAN UNION, 2005a; 2005b 참조).

34) 여러 국가들에서 전자 국가신분증에 대한 거부 역사가 유구하다. 프랑스는 1979년 말 내무부에서 컴퓨터로 읽을 수 있는 형태의 개인카드시행계획을 세운 적이 있었지만, 다른 목적으로 이용될지 모른다는 사회적 격론이 일었고 1981년 9월 새로 취임한 사회당 미테랑 정부는 개인확인카드의 도입을 포기하였다. 2003년에 다시 전자신분증의 도입이 추진되었으나, 생체정보 입력에 대한 반대여론에 부딪혀 이 계획도 보류되었다(고문현 외, 2010). 호주는 1985년 탈세 방지, 복지 행정, 불법이민확산방지 등을 이유로 전자적 방식의 오스트레일리아 카드를 도입하려는 계획이 발표되자 비판이 일었고, 정부기관인 뉴사우스웨일즈프라이버시위원회도 카드 계획안이 단순한 신원 확인 이상의 문제이고 정부에로의 권력과 권위의 집중화 수단으로서 호주에서의 자유에 대한 중대한 위협을 내포하고 있다는 점을 경고하였다. 결국 1987년 대중의 거대한 저항과 정당의 반란, 시민들의 불복종에 직면한 정부는 카드 입법안을 폐기하였다. 그밖에도 필리핀, 뉴질랜드 등에서 전자주민증 반대 운동이 있었음이 보고되고 있다(임영화, 1997).

네덜란드는 의무발급이 아니고 의무발급에 대한 저항감이 상당하다(Whitley, 2005; 2009). 스웨덴은 의무발급이 아니고 지문을 수록하지 않는다. 주민등록번호와 유사한 개인식별번호를 가지고 있지만 사용처가 사회보장 서비스전달 등으로 제한되어 있다(권건보, 2005; 송희준 외, 2007; 고문현 외, 2010) 핀란드 역시 의무발급이 아니고 지문을 수록하지 않는다.

벨기에는 지문을 수록하지 않는다. 데이터베이스는 분산형이다(Statewatch, 2011). 에스토니아는 지문을 수록하지 않는다. 특히 포르투갈은 헌법 제35조 제3항에서 “시민들에게 다목적의 국민식별번호가 부여되어서는 안 된다”고 규정함으로써 표준통일식별번호의 도입을 명시적으로 금지하고 있다(고문현 외, 2010).

일본은 국가신분증을 전국단위에서 의무발급하지 않고 지자체별로 자율발급한다. 일본의 주민관리업무는 전적으로 자치단체 소관으로서 시·정·촌의 주민정보는 상호 교류되지 않는 것을 원칙으로 하고 있고, 중앙행정부처와 도·도·부·현의 지사는 소관사무에 필요한 경우에 한하여 시·정·촌에 자료제공을 요청할 수 있을 뿐이다. 주민기본대장 네트워크 시스템의 도입에 따라 IC칩이 내장된 주민기본대장카드가 발급되고 있지만 주민본인의 선택에 따라 자치단체에서 발급된다. 번호의 일종인 주민표 코드는 해당주민의 신청에 따라 언제든지 변경할 수 있고, 법령에서 정하는 사무처리용도 외로 요구하거나 이용할 수 없으며 민간 이용이 제한된다. 지문도 수록하고 있지 않다(고문현 외, 2010).

결국 전자주민증을 도입한 OECD 국가 중에서도 의무발급, 주민등록번호, 지문날인 제도를 모두 가지고 있는 경우는 극히 일부에 불과하다. 전자주민증을 도입한 많은 국가들의 경우에도 선택발급하고 있다. 나머지 OECD 23개국은 전자주민증을 도입하고 있지 않다. 특히 테러 방지 등의 명분으로 영국이 최근까지 전자주민증을 추진하였으나 프라이버시 침해와 예산 논란 끝에 2010년 12월 관련 법률을 공식적으로 폐지하였다는 사실에 주목할 필요가 있다.

전 국민을 대상으로 신분증 발급, 주민등록번호 부여, 지문날인 제도를 모두 의무적으로 시행하는 데에다 국민 대다수의 주민등록번호가 인터넷에 기유출된 한국에서 전자주민증을 도입하면서 선택으로 삼을 만한 국가는 거의 없는 것이다. 이러한 상황에서 한국이 전자주민증을 도입하면 국민에게 미치는 침해성이 세계 유례 없는 수준일 것이다.

VI. 결론

전자주민증 도입 예산으로 정부는 10년 간 4,862억 원을 추계하였지만, 누락된 것으로 추정되는 비용을 합산하면 1조 원 가까이 소요될 것으로 보인다(민주주의법학연구회, 2011)³⁵⁾. 투입될 비용에 비해 전자주민증 도입의 목적과 수단이 타당한지 의구심을

35) “주민증 분실분 차액 113억 원+정부부담 판독기 구입비용 차액 93억 원+민간부담 판독기 구입비용 차액 350억 원+10년 동안의 판독기 재구입비용(정부부담+민간부담) 974억 원=1530억 원의 추가비용이 계산된다. 따라서 정부가 산정한 총 예산 4862억 원에다 추가비용 1530억 원을 더하면, 총 6392억 원의 예산이 필요할 것으로 판단된다 ... 만약 좀 더 현실성이 있어 보이는 전자공무원증의 발급단가를 반영하면 ... 그 예산이 무

찾지 않을 수 없다.

행정안전부가 인권시민단체의 우려를 해소하기 위해 수정안을 제시했다고 하나, 주민등록법 개정안 및 수정안은 전자주민증 도입의 충분한 근거가 되기에 부족하다. 주민등록증의 경신 필요성은 전자기능 도입의 근거가 될 수 없고, 주민등록번호와 지문을 보호하기 위한 방법은 전자칩 수록이 아니라 정보 삭제에 대한 재고여야 한다. 전자신분증이 위·변조에 늘 안전할 것이라고 장담하기도 어렵다. 현재 제시된 법안으로는 통합신분증과 네트워크 연동 가능성을 배제할 수 없다는 점에서 향후 전자주민증의 확장도 우려되는 상황이다.

무엇보다 주민등록제도에 대한 근본적인 재고가 필요한 시점이다. 주민등록번호와 지문 수록, 그리고 주민등록증의 의무발급 제도는 집약적인 인권침해이다. 이미 현행 주민등록증도 주민등록제도의 입법취지와 목적을 넘어서 과도하다는 지적이 있어온 마당에 전자적 방식으로 개인정보가 유출되고 오남용될 위험성을 방지할 길은 도입하지 않는 것뿐이다.

정부가 이 민감한 제도를 도입하는 과정에서 보여준 일방적인 태도는 시민사회에서 이미 신뢰를 잃었다³⁶⁾. 정부의 막연한 장담과 기술적 낙관을 근거로 전자주민증을 도입하기에는 너무 많은 위험을 감수해야 한다. 전자주민증 도입 법안은 폐기되어야 마땅하다.

<참고 문헌>

감사원, 2008, “감사결과 처분요구서: 행정정보 공유 및 관리실태”, 2008. 5.

건강권실현을위한보건의료단체연합, 2010, “혈액형 기입을 빌미로 도입하려는 전자주민증에 반대한다”, 2011. 3. 8.

경제정의실천시민연합, 2011, “전자주민증은 개인정보보호를 위한 정책에 역행하는 것이다”, 2011. 9. 6.

고문현·류시조·권건보·김주영·고문철·이남경, 2010, 「국가신분확인체계 발전방안연구」, 사단법인 한국비교공법학회, 행정안전부 지원, 2010. 12.

국회 행정안전위원회 수석전문위원, 2010, “전자주민증 갱신에 따른 소요비용 추산”, 주민등록법 일부개정법률안 검토보고서, 2010. 11.

권건보, 2005, 『개인정보보호와 자기정보통제권』, 경인문화사.

권건보, 2010, “전자주민증 도입방안의 헌법적 검토”, 사단법인 한국 공법학회, 「공법연구」 제39집 제2호, 2010. 12.

려 9,825억 원에 다다르게 된다. 거의 1조 원에 육박하는 비용이다!”(민주주의법학연구회, 2011).

36) 행정안전부는 관련 입법 예고를 3차례나 하는 과정에서도 전자주민증을 추진하는 사실을 투명하게 공개하거나 공청회를 갖지 않았다. 갑작스런 입법예고 후 2달 만에 국회 법안 발의를 강행하여 불신을 자초하였다(참세상, 2010; 김주영, 2011).

권건보, 2011, “‘마이너리티 리포트’ 현실 되나”, 「인권」 통권 70호, 국가인권위원회, 2011 9·10.

김민호·지성욱·김명식, 2009, 「주민등록번호제도 개선방안연구」, 성균관대학교 산학협력단, 국가경쟁력강화위원회 지원, 2009. 11.

김일환, 2005, “個人識別番號(住民登録番號)의 違憲性與否에 관한 考察”, 국가인권위원회 주최 토론회 「주민등록번호제도 이대로 좋은가?」, 2005. 4. 6.

김주영, 2011, “전자주민증 도입방안에 대한 비판적 검토: 2010년의 『주민등록법』 개정안을 중심으로”, 사단법인 한국 공법학회, 「공법연구」 제39집 제3호, 2011. 2.

김호연, 2011, “외교부, 전자여권 개인정보 유출 축소 및 은폐 의혹!”, 김호연 의원실 2011년 국정감사 보도자료, 2011. 9. 19.

뉴스라이브, 2008, “송영선 ‘20만원짜리 판독기로 개인정보 술술’”, 2008. 10. 7, <<http://www.newslive.co.kr/news/article.html?no=29502>>, 검색일: 2011. 8. 31.

뉴시스, 2008, “<국감>진수희 ‘IC카드 복제 가능…금융사고 위험 노출’”, 2008. 10. 2, <<http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=003&aid=0002337337>>, 검색일: 2011. 8. 31.

뉴시스, “‘나도 모르게 내 정보가…’ 갈수록 개인정보 유출피해”, 2011. 4. 23, <<http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=003&aid=0003817153>>, 검색일: 2011. 8. 31.

다산인권센터·문화연대·민주사회를위한변호사모임·불교인권위원회·울산인권운동연대·인권연대·인권운동사랑방·제주평화인권센터·진보네트워크센터·천주교인권위원회·청소년인권행동 ‘아수나로’·청소년인권활동가네트워크·함께하는시민행동, 2010, “전자주민증 관련 ‘주민등록법’ 개정안에 대한 인권시민단체 공동의견서” 및 “기자회견문 : 감시통제사회를 완성하는 전자주민증 도입을 반대한다!”, 2010. 10. 14, <<http://act.jinbo.net/drupal/node/6229>>, 검색일: 2011. 8. 31.

동아일보, 2011, “공공기관 개인정보 과다보유: 경찰자료 2000년 이후 고스란히… 지워지지 않는 ‘주홍글씨’”, 2011. 2. 15.

민주주의법학연구회, 2011, “전자주민증 관련 ‘주민등록법’ 개정안에 대한 민주주의법학연구회 의견서”, 2011. 6.

송희준·김종철·조동섭·김상운·김현귀, 2007, 「주민등록제도 발전방안 연구」, 행정자치부 지원, 2007. 12.

심우민, 2011, “네이트 해킹사고와 포털의 개인정보보호”, 「이슈와 논점」 제282호, 국회 입법조사처, 2011. 8. 9.

연합뉴스, 2011, “공공기관 정보유출 46%, 공무원 부주의 탓”, 2011. 9. 20.

오길영, 2011, “전자주민증 도입의 쟁점과 함의”, 「민주법학」 제46호, 2011. 7.

이민영, 2010, “정보인권의 법적 의의와 좌표”, 『정보인권의 법적 보장과 그 구체화 공동학술세미나』, 국가인권위원회, 2010. 12. 23.

이인호, 2009, 「정보인권의 개념과 헌법적 보장체계」, 국가인권위원회.

이재경, 2011, “독일의 전자신분증 제도”, 「최신외국법제정보」 2011년 제3호, 한국법제연구원, 2011. 6.

인도주의실천의사협의회, 2011, “주민등록법 개정안에 대한 인도주의실천의사협의회 의견서”, 2011. 1.31.

임영화, 1997, “호주의 ID카드 반대운동”, 「이달의 민변」 1997년 7월호.

임헌만, 2005, “전자주민카드 정책과정상의 프라이버시 이슈와 교훈”, 「한국사회와 행정연구」 제16권 제3호, 2005. 11.

전성배, “인터넷상의 주민번호 보호 방안 검토”, 국가인권위원회 주최 토론회 「주민등록번호제도 이대로 좋은가?」, 2005. 4. 6.

조화순, 2005, “정보사회의 국가권력과 개인정보: 한국의 전자주민카드 도입논의를 중심으로”, 「한국정치학회보」 제39권 2호, 2005. 6.

참세상, 2010, “전자주민증, 5월에 국민 몰래 도입하려다 무산”, 2010. 7. 9. <<http://www.newscham.net/news/view.php?board=news&nid=57603>>.

참여연대, 2011, “행정안전부 제출 주민등록법일부개정법률안(2010.9.20.의안번호 9418)의 행정안전부 수정안(2011.3)에 대한 참여연대 검토 의견”, 2011. 6. 23.

한국전산원, 1996, “전자주민카드의 제작 및 운영에 관한 연구”, 1996. 12, 201면이하; 민주사회를위한변호사모임, “인권관련 개혁 제안서”, 1998. 2. 16, <<http://go.jinbo.net/commune/view.php?board=nocard-2&id=804&page=1>>, 검색일: 2011. 8. 31.

행정안전부, 2010a, “해명자료”, 2010. 9. 15, <<http://www.mopas.go.kr/gpms/ns/mogaha/user/userlayout/bulletin/bonbu/admi/userBtView.action?userBtBean.bbsSeq=1019960&userBtBean.ctxCd=1281&userBtBean.ctxType=21010002&searchKey=1&searchVal=¤tPage=1>>, 검색일: 2011. 4. 15.

행정안전부, 2010b, “공청회 개최('10.10.25) 관련 자료제공 : 전자주민등록증 도입 공청회 개최계획 및 참고자료”, 2010. 10.

행정안전부, 2010c, “주민등록법 일부개정법률안 정부 개정안(수정)”, 2010. 12.

행정안전부, 2011a, “전자주민등록증의 IC칩 정보 열람 방법”, 2011. 2.

행정안전부, 2011b, “전자주민증 관련 주민등록법 수정의견 검토”, 2011. 3.

행정안전부, 2011c, “전자주민등록증 도입 추진방안”, 2011. 3, <<http://www.mopas.go.kr/gpms/view/jsp/download/userBulletinDownload.jsp?userBtBean.bbsSeq=1019958&userBtBean.ctxCd=1281&userBtBean.orderNo=1>>, 검색일: 2011. 4. 15.

행정안전부, 2011d, “전자주민등록증 관련 시민단체 주장 검토”, 2011. 4.

행정안전부, 2011e, “전자주민등록증 관련 시민단체 주장 검토”, 2011. 6.

행정안전부, 2011f, “설명자료”, 2011. 8. 9,

<<http://www.mopas.go.kr/gpms/ns/mogaha/user/userlayout/bulletin/userBtView.action?userBtBean.bbsSeq=1020661&userBtBean.ctxCd=1013&userBtBean.ctxType=21010002&Page=1>>, 검색일: 2011. 8. 31.

행정안전부, 2011g, “11. 8. 11, 당정협의자료 : 최근 개인정보 유출사고에 따른 개인정보보호 종합대책”, 2011. 8. 11.

행정정보공유추진위원회, 2011, “제출하지 않아도 되는 구비서류: 주민등록표 등·초본”, <<http://pr.share.go.kr/fa/fa010/ehanaro/table/1.jsp>>, 검색일: 2011. 8. 31.

COUNCIL OF THE EUROPEAN UNION, 2005a, "Draft Conclusions of the Representatives of the Governments of the Member States on common minimum security standards for Member States' national identity cards", 2005. 11. 11, , <<http://www.statewatch.org/news/2005/nov/eu-biometric-ID-Cards-Conclusions.pdf>>, 검색일: 2011. 8. 31.

COUNCIL OF THE EUROPEAN UNION, 2005b, "PRESS RELEASE: Main results of the Council", 2005. 12. 1-2, <<http://www.consilium.europa.eu/uedocs/cmsUpload/JHA,1-2.12.05.pdf>>, 검색일: 2011. 8. 31.

ENISA, 2009, "Privacy and Security Risks when Authenticating on the Internet with European eID Cards", 2009. 11. 26, <http://www.enisa.europa.eu/act/it/eid/eid-online-banking/at_download/fullReport>, 검색일: 2011. 8. 31.

Information Commissioner's Office, 2005, “The Identity Card bill - the information commissioner's concerns”, 2005. 10, <http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_concerns_october_2005.pdf>, 검색일: 2011. 8. 31.

Statewatch, 2011, “Statewatch Briefing: ID Cards in the EU: Current state of play”, <<http://www.statewatch.org/analyses/no-107-national-ID-cards-questionnaire.pdf>>, 검색일: 2011. 8. 31.

Whitley, Edgar A, et al., 2005, “The Identity Project: An assessment of the UK Identity Cards Bill & its implications”, The London School of Economics and Political Science, 2005. 3, <

http://www2.lse.ac.uk/intranet/LSEServices/ERD/pressAndInformationOffice/PDF/ID_report_updated.pdf>, 검색일: 2011. 8. 31.

Whitley, Edgar A, and Hosein, Gus, 2009, *Global Challenges for Identity Policies*, Palgrave Macmillan.

Wikipedia, 2011a, “Identity document”, <http://en.wikipedia.org/wiki/Id_card>, 검색

색일: 2011. 8. 31.

Wikipedia, 2011b, “List of national identity card policies by country”,
<http://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country>,

검색일: 2011. 8. 31.

<별첨>

【개정안과 수정안 조문 대비표】

현행	개정안	수정안
제24조(주민등록증의 발급 등) ① (생략)	제24조(주민등록증의 발급 등) ① (현행과 같음)	제24조(주민등록증의 발급 등) ① (현행과 같음)
② 주민등록증에는 성명, 사진, 주민등록번호, 주소, 지문(指紋), 발행일, 주민등록기관을 수록한다. 다만, 혈액형에 대하여는 대통령령으로 정하는 바에 따라 주민의 신청이 있으면 추가로 수록할 수 있다.	② 주민등록증에는 다음 각 호의 사항을 수록한다. 이 경우 제10호의 유효기간의 설정에 대해서는 대통령령으로 정한다. 1. 성명 2. 성별 3. 생년월일 4. 주소 5. 사진 6. 주민등록번호 7. 지문(指紋) 8. 발행일 9. 발행번호 10. 유효기간. 다만, 주민등록증의 발급 또는 재발급 당시의 연령 등을 고려하여 대통령령으로 정하는 사람에 대해서는 적용하지 아니한다. 11. 주민등록기관 12. 혈액형 등 대통령령으로 정하는 사항 중 주민의 수록신청이 있는 것	② 주민등록증에는 다음 각 호의 사항을 수록한다. 이 경우 제10호의 유효기간의 설정에 대해서는 대통령령으로 정한다. 1. ~ 11. (개정안과 같음) 12. 혈액형. 다만, 대통령령으로 정하는 바에 따라 주민의 수록신청이 있는 경우에 한한다.
		③ 제2항제9호의 주민등록증 발행번호는 개인의 특성을 파악하거나 유추할 수 없는 형태로 부여하여야 한다.
<신설>	③ 시장·군수 또는 구청장은 제10조의2제1항에 따라 신고	④ (개정안 제3항과 같음)

현행	개정안	수정안
	한 국외이주국민에게 발급하는 주민등록증에는 대통령령으로 정하는 방법으로 국외이주국민임을 추가로 표시하여야 한다.	
<신 설>	④ 제2항 및 제3항에 따라 주민등록증에 수록되거나 표시되는 정보는 전자적으로 수록할 수 있다. 이 경우 전자적 수록의 방법, 전자적으로 수록된 정보의 타인에 대한 제공 또는 열람 방법, 보안조치 등에 관하여 필요한 사항은 대통령령으로 정한다.	<삭 제>
제24조의2 <신 설>		제24조의2(주민등록증 정보의 전자적 수록 등) ① 제24조제2항 및 제4항에 따라 주민등록증에 수록되거나 표시되는 정보는 주민등록증의 위조 및 변조를 방지하고 개인정보를 보호하기 위하여 전자적으로 수록할 수 있다
		② 행정안전부는 제1항에 의하여 전자적으로 수록하는 주민등록증을 제작하여 보급하는 경우에는 사전에 개인정보 보호에 미치는 영향과 기술적 안정성을 평가하여야 한다.
		③ 제24조 제2항 각호에 따라 주민등록증에 수록된 정보 중 전자적으로만 수록된 정보를 판독기(전자적으로 수록된 정보를 열람하는 전산장비를 말한다. 이하 같다)를 통하여 열람하는 경우에는 사전에 본인의 동의를 얻어야 한다.

[illegible]

부 칙

제1조(시행일) 이 법은 공포 후 1년이 경과한 날부터 시행한다.

제4조 (주민등록증 발급에 관한 특례) ① 제24조제2항 및 제4항의

개정규정에 따른 새로운 주민등록증의 발급 및 사용에 관한 사항은 새로운 주민등록증의 발급 준비상황을 고려하여 대통령령으로 정하는 바에 따라 순차적으로 적용하되, 2017년 12월 31일까지 제24조제2항 및 제4항의 개정규정에 따른 새로운 주민등록증 발급을 전국적으로 완료하여야 한다.

② 제1항에 따라 새로운 주민등록증 발급이 전국적으로 완료된 후에는 종전의 제24조제2항에 따른 주민등록증을 사용할 수 없다.

③ 제1항에 따라 새로운 주민등록증을 발급받기 전까지는 종전의 제24조제2항에 따른 주민등록증을 사용할 수 있다.