

헌법소원심판청구서

청구인

청구취지

“정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의2 제1항 제1호는 헌법에 위반된다.”

라는 결정을 구합니다.

침해된 권리

개인정보자기결정권

침해의 원인

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의2 제1항 제1호

청구이유

I. 사건의 개요

1. 청구인의 지위

청구인은 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법"이라 합니다)상 본인확인기관인 주식회사 케이티의 이동통신 서비스를 이용하는 자로서 2010. 6. 30. 회원 가입 시 주식회사 케이티에 주민등록번호를 제공한 자입니다.

2. 사건의 경과

청구인은 주식회사 케이티의 이동통신서비스를 이용하기 위해 주식회사 케이티에 주민등록번호를 제공하였습니다. 주식회사 케이티가 2012. 12. 28. 본인확인기관으로 지정되어 정보통신망법 제23조의2 제1항 본문의 예외에 해당하여 청구인의 주민등록번호를 계속 수집 보관하고 있던 도중 2014. 3. 해킹을 당해 청구인의 주민등록번호를 포함한 개인정보가 유출되었습니다. 당해 개인정보 유출사건으로 인하여 청구인을 포함한 1,200만명의 개인정보가 유출된 바 있습니다.

청구인은 2014. 5. 19. 주식회사 케이티의 홈페이지를 통해 자신의 주민등록번호가 유출되었다는 것을 확인하였고, (청구인의 개인정보 유출내역은 첨부서류 1 참조) 주식회사 케이티가 아닌 다른 이동통신서비스 사업자(본인확인기관)에 주

민등록번호를 제공하지 않고 서비스 이용계약을 체결하려고 했으나 주민등록번호 제공 없이는 어떠한 이동통신 서비스에도 가입할 수 없었습니다.

3. 청구대상 법률조항

정보통신망법 제23조의2(주민등록번호의 사용 제한)

① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우

II. 헌법소원심판의 요건

1. 자기관련성, 직접성, 보충성

(1) 자기관련성

정보통신망법 제23조의2 제1항 본문은 정보통신서비스 제공자에게 원칙적으로 주민등록번호를 수집·이용할 수 없도록 규율하고 있습니다. 그러나 정보통신망법 제23조의2 제1항 제1호(이하 “이 사건 법조항”이라 합니다)는 본인확인기관에 예외적으로 주민등록번호를 수집·이용할 수 있는 권리를 부여하고 있습니다. 이 사건 법조항에 따라 주민등록번호를 본인확인기관에 제공해야 하는 실질적인 의무는 본인확인기관을 이용하는 이용자에게 부과되므로, 그 규제의 법적 구조는 법 규정 - 본인확인기관 - 이용자의 삼각구도로 짜여 있어, 정보통신망을 통해 청구인과 같은 이용자의 주민등록번호가 수집, 유통됨으로써 실질적으로 기본권

을 침해받는 자는 이용자가 되는 구조입니다.

(2) 직접성

헌법소원 심판의 대상이 될 수 있는 법률은 그 법률에 기한 다른 집행행위를 기다리지 않고 직접 국민의 기본권을 침해하는 법률이어야 하나, 구체적 집행행위가 존재하는 경우라고 하여 언제나 반드시 법률자체에 대한 헌법소원심판청구의 적법성이 부정되는 것은 아니며, 예외적으로 집행행위가 존재하는 경우라도 그 집행행위를 대상으로 하는 구체절차가 없거나 구체절차가 있다고 하더라도 권리구제의 기대가능성이 없고, 다만 기본권 침해를 당한 청구인에게 불필요한 우회절차를 강요하는 것밖에 되지 않는 경우 등으로서 당해 법률에 대한 전제 관련성이 확실하다고 인정되는 때에는 당해 법률을 헌법소원의 직접 대상으로 삼을 수 있다(헌재 1992. 4. 14. 90헌마82, 판례집 4, 194, 203; 헌재 1997. 8. 21. 96헌마 48, 판례집 9-2, 295, 303-304)고 할 것입니다.

이 사건 법조항의 경우 본인확인기관으로 지정된 주체에 다른 집행행위를 기다리지 않고 바로 주민등록번호를 수집, 이용할 권한을 부여하고 있어 청구인의 기본권을 직접 침해하는 구조이므로 당해 법률을 헌법소원의 직접 대상으로 삼을 수 있다고 할 것입니다.

한편 방송통신위원회의 본인확인기관 지정행위가 행정청에 의한 집행행위에 해당할 여지가 있으나, 청구인들이 본인확인기관 지정행위에 대한 취소소송을 통한 권리구제의 기대가능성이 거의 없고, 기본권 침해를 당한 청구인에게 불필요한 우회절차를 강요하는 것에 해당하므로 이 사건 청구는 직접성의 요건을 충족합니다.

(3) 보충성

헌법재판소법 제68조 제1항 후단은 “다른 법률에 구제절차가 있는 경우에는 그 절차를 거친 후가 아니면 청구할 수 없다.”라고 규정하고 있는데, 이 사건 법조항의 위헌 여부를 다투는 본 심판청구에 있어서 법률의 효력을 소송물로 일반법원에 소를 제기하여 구제받을 수 있는 절차가 존재하지 않는다고 할 것입니다.

2. 청구기간

법령에 대한 헌법소원의 청구기간은 그 법령의 시행과 동시에 기본권을 침해당한 자는 그 법령이 시행된 시점을 기준으로, 법령이 시행된 후 비로소 그 법령에 해당하는 사유가 발생하여 기본권의 침해를 받게 된 경우에는 그 사유가 발생한 시점을 기준으로 하여야 할 것이며, 법령시행일을 청구기간 기산일로 하는 것이 기본권 구제의 측면에서 부당하게 청구기간을 단축하는 결과가 되거나, 침해가 확실히 예상되는 때로부터 기산한다면 오히려 기산일을 불확실하게 하여 청구권의 유무를 불안정하게 하는 결과를 가져올 경우 등에는, 법령시행일이 아닌 법령이 적용될 해당사유가 발생하여 기본권침해가 비로소 현실화된 날부터 기산함이 상당하다고 할 것입니다.

이 사건 법조항이 개정 시행된 이후인 2012. 12. 28. 에야 방송통신위원회가 주식회사 케이티를 포함한 이동통신사들을 본인확인기관으로 지정하였으며, 주식회사 케이티가 청구인의 주민등록번호를 수집·이용하고 있던 도중인 2014. 3. 경 주민등록번호를 유출하면서 비로소 청구인의 기본권 침해 사유가 발생한 경우에 해당합니다.

한편 청구인은 청구인은 2014. 5. 19. 주식회사 케이티의 홈페이지(kt.com)를 통해 주민등록번호를 포함한 청구인의 개인정보 유출 여부를 알게 되었고, 이에 곧

바로 주식회사 케이티가 아닌 다른 본인확인기관을 통해 주민등록번호의 제공 없이 이동통신 서비스 계약을 체결하려고 했으나 계약을 체결할 수 없었습니다. 따라서 청구인은 2014. 5. 19. 경에야 이 사건 법조항으로 인한 기본권 침해 사유가 발생한 것을 알게 되었다고 보아야 하며, 이 사건 청구서 제출일 현재 기본권 침해사실을 알게된 지 90일이 도과하지 않았습니다.

III. 주민등록번호 제도의 현황

1. 주민등록번호 제도의 특성

주민등록제도는 1962년 제정된 주민등록법에 의해 도입되었고, 주민등록번호는 1968년 주민등록법 제1차 개정 시 추가된 주민등록증 제도와 함께 도입되었습니다.

주민등록번호는 운전면허증이나 다른 고유식별번호와는 달리 본인의 의사와는 무관하게 출생과 동시에 강제적으로 모든 국민에게 부여되며, 한번 국민에게 부여된 주민등록번호는 예외적인 사유가 아닌 이상 변경이 불가능 합니다.

주민등록증은 “간첩이나 불순불자를 용이하게 식별, 색출하여 반공태세를 강화하기 위하여” 도입되어 1975년 생년월일, 성별, 지역을 표시하는 13자리의 숫자체제로 정착되었는데, 당시 이에 대하여 ‘인간에게 번호를 붙여 인간의 존엄성을 해친다,’ ‘개인을 국가 행정편의의 도구처럼 희생시킨다’는 비판이 제기되기도 하였습니다.

이러한 목적 하에서 도입된 주민등록번호는 현재까지 공공행정 뿐 아니라 민간의 각종 법률관계에서도 개인의 신원을 증명하는 고유식별정보로 사용되고 있습니다. 특히 공공기관의 본인확인 뿐 아니라 민간에서도 회원가입 시 주민등록번호를 요구하고 있었으며, 현대의 정보통신기술의 발달과 맞물려 개인정보를 포함한 고객

정보시스템 구축 및 시스템간의 연계에서 주민등록번호는 주요 키(key) 값으로 사용되고 있습니다. 그러나 개인정보취급자의 정보의 무단수집과 관리소홀, 악의적 유출, 제3자의 해킹 및 시스템의 설계 오류 등으로 주민등록번호를 비롯한 민감한 개인정보가 지속적으로 유출되면서 그 피해가 나날이 커지고 있는 상황입니다.

이렇듯 주민등록번호는 전 국민을 하나의 개인식별번호체계로 파악하면서 정보화 사회의 진전과 함께 점차 그 사용이 증가하게 되었고, 주민등록번호를 통해 보관되거나 파악할 수 있는 개인정보의 양이 급속도로 축적되면서 개인정보의 침해 및 유출 등 피해 사례가 끊임없이 발생하고 있습니다. 이동통신사 외에도 대형 포털사이트, 금융회사, 온라인 쇼핑몰 등에 대한 연이은 해킹사건 발생하고 있는 것입니다. 이로 인해 대규모로 유출된 개인정보를 이용한 명의도용, 스팸, 전화사기 등 2차 피해에 국민들의 불안감이 확산되고 있는 등, 그 유출로 인한 피해는 오롯이 국민들이 전적으로 부담하고 있습니다.

2. 주민등록번호 수집금지 원칙

(1) 개인정보자기결정권의 의의

가. 개인정보자기결정권의 개념

새로운 독자적 기본권으로서의 개인정보자기결정권을 헌법적으로 승인할 필요성이 대두된 것은 다음과 같은 사회적 상황의 변동을 그 배경으로 한다고 할 수 있습니다. 이에 대해 헌법재판소는 아래와 같이 판시하였습니다.

“인류사회는 20세기 후반에 접어들면서 컴퓨터와 통신기술의 비약적인 발전에 힘입어 종전의 산업사회에서 정보사회로 진입하게 되었고, 이에 따른 정보환경의 급격한 변화로 인하여 개인정보의 수집·처리와 관련한 사생활보호라는 새로운 차원의 헌법문제가 초미의 관심사로 제기되었다.

현대에 들어와 사회적 법치국가의 이념 하에 국가기능은 점차 확대되어 왔고, 이에 따라 국가의 급부에 대한 국민의 기대도 급격히 높아지고 있다. 국가가 국민의 기대에 부응하여 복리증진이라는 국가적 과제를 합리적이고 효과적으로 수행하기 위해서는 국가에 의한 개인정보의 수집·처리의 필요성이 증대된다. 오늘날 정보통신기술의 발달은 행정기관의 정보 수집 및 관리 역량을 획기적으로 향상 시킴으로써 행정의 효율성과 공정성을 높이는 데 크게 기여하고 있다. 이와 같이 오늘날 국민이 급부행정의 영역에서 보다 안정적이고 공평한 대우를 받기 위해서는 정보기술의 뒷받침이 필연적이라고 할 수 있다.

한편, 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. 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 낱알이 파악할 수 있게 되었다.

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 보장장치라고 할 수 있다.”

(헌법재판소 2005. 5. 26. 99헌마513 등, 주민등록법 제18조의8 등 위헌확인)

이렇게 확대된 권리는 “자신과 관계된 정보의 흐름을 통제하는 권리(individual right to control the circulation of information relation to oneself),” “언제 어떠한 한계들 내에서 개인적 생활을 공개할 것인지를 원칙적으로 스스로 결정하는, 개인적 자기결정의 사상에서 나오는 권리,” “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 권리”로 정의되고, 이것이 바로 개인정보자기결정권, 자기정보관리통제권, 자기정보통제권, 등으로 불리게 되었습니다. 그리하여 개인정보자기결정권의 배경에는 자기에 대한 정보가 타인에 의하여 함부로 이용되지 않는 것이, 개인의 행복추구를 위하여 불가결하다는 인식이 있으며, 또 그것이 현대의 정보사회에서 대부분의 사람에게 받아들여지는 것은 부정할 수 없을 것입니다.¹

한편 헌법재판소는 개인정보자기결정권의 보호대상이 되는 개인정보에 대해 “개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않

¹ <개인정보자기결정권의 제한과 전자여권>, 이상명, 법학논총, 한양대학교 법학연구소 (2008) pp.159-160

고 공적 생활에서 형성되었거나 이미 공개된 정보까지 포함한다”²고 정의한 바 있습니다. 따라서 이 사건 청구에서 문제되는 ‘주민등록번호’는 개인의 동일성을 가장 완벽하게 식별할 수 있는 정보에 해당하므로 주민등록번호는 개인정보자기결정권의 보호대상이 된다고 할 것입니다.

나아가 헌법재판소는 정보사회로의 급격한 진입으로 개인정보의 수집·처리와 관련한 사생활 보호라는 새로운 차원의 헌법문제가 야기되었고, 그에 따라 개인정보자기결정권을 새로운 독자적 기본권으로서의 ‘개인정보자기결정권’을 헌법적으로 승인할 필요가 있다고 하였습니다. 그리고 이것이 “현대의 정보통신 기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치”라고 설명하고 있습니다.

나. 개인정보자기결정권의 구체적인 내용³

일반적으로 개인정보자기결정권의 내용은 다음과 같습니다.

첫째, 정당한 수집목적을 위하여, 필요한 범위 내에서, 공정하고 합리적인 방식으로, 정보주체의 분명한 인식 또는 동의 하에 수집되어야 하는 수집제한청구권이며, 수집목적의 정당성, 수집범위의 필요 최소성, 수집방식의 합리성, 정보주체의 인식명확성 등의 요건에 대한 판단은 이익형량을 통해 결정되어야 할 것입니다.

둘째, 기본적인 정보처리 원칙이 충족되지 않는 경우에는 개인정보의 이용·제공

² 헌법재판소 2005. 5. 26., 99헌마513 등, 주민등록법 제18조의8 등 위헌확인

³ <개인정보자기결정권의 제한과 전자여권>, 이상명, 법학논총, 한양대학교 법학연구소 (2008) pp.160 -161

등의 정보처리를 금지하도록 요구할 수 있는 정보처리금지청구권이며, 여기에는 이용제한요구권, 시스템공개요구권 등이 있습니다

셋째, 타인에 의하여 처리되고 있는 개인정보의 내용에 대하여 정보주체가 자신에 관한 정보의 열람을 청구할 수 있는 정보열람청구권(정보접근권)입니다.

넷째, 정보주체가 자신에 관한 정보를 열람한 결과 정보내용이 부정확하거나 불완전한 것일 경우 이에 대한 정정을 요구할 수 있는 권리인 정보정정청구권이며, 정보주체의 정정요구가 있을 경우 정보보유기관은 잘못된 부분을 정정하고 정보주체에게 그 사실을 통보해야 합니다.

다섯째, 개인정보 제공자가 정보보유기관에 대해 자신의 정보에 대한 일반인이나 그 밖에 권한 없는 자의 불법적인 접근을 지속적으로 막아줄 것을 요구할 수 있는 정보차단청구권입니다.

여섯째, 특정목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 원칙적으로 통합되지 않고 분리된 상태로 유지될 것을 요구할 수 있는 정보분리청구권입니다.

일곱째, 정보보유기관이 법에 규정된 의무를 위반하거나 법의 취지에 반하여 개인정보를 부당하게 이용할 경우 정보주체가 자기정보의 삭제를 요구할 수 있는 정보삭제청구권입니다.

다. 고유식별번호 수집 제한의 원리

개인정보가 고유식별번호인 경우에는 개인정보자기결정권의 보호법익은 훨씬 더 긴절해집니다. 고유식별번호란 국가가 복지, 세무 등의 행정 목적으로 모든 국민을 고유하게 식별하기 위해 부여하는 번호를 말합니다. 고유식별번호는 거의 모든 국민에게 부여되고 고유한 식별력을 가지기 때문에 민간기업들은 이를 영업상 고객식별목적으로 이용하고자 하는 강한 동기를 갖게 됩니다. 그러나, 민간기업들이 이렇게 할 경우, 이 고유식별번호를 연결고리로 하여 수많은 개인정보들이 유출되거나 집합될 수 있는 위험이 발생합니다. 결국 이렇게 데이터들이 집적될 경우 한 개인에 대한 전방위적인 감시가 가능해지고 감시당하는 자는 실질적인 자유를 누리지 못하게 됩니다.

이런 이유로 우리나라에서 전 국민에게 강제적으로 부여되는 개인식별번호인 주민등록번호는 개인정보자기결정권 상 보호가치가 매우 크다고 할 것입니다. 즉, 주민등록번호 제도의 위험성에 비례하여 주민등록번호의 도입목적 외 사용은 엄격하게 제한되어야 하는 것이며, 이에 따라 공공행정 영역이 아닌 민간 영역의 주민등록번호 수집제한청구권이 강하게 요구됩니다.

이에 따라 우리나라에서 보편적으로 개인정보자기결정권을 보호하는 법이라고 할 수 있는 개인정보보호법은 제24조에서 고유식별번호는 정보주체의 동의가 있더라도 다른 법령이 수집을 허용하거나 요구하지 않는 한 금지하고 있습니다. 정보통신서비스제공자들이 수집하는 개인정보와 관련하여 개인정보자기결정권을 보호하는 법이라고 말할 수 있는 정보통신망법 제23조의2 제1항 본문에 규정된 “정보통신서비스 제공자에 대한 주민등록번호 수집금지 의무”는 주민등록번호 제도가 배태하고 있는 위험성을 고려하여 개인정보자기결정권의 내용 중 하나인 ‘수집제한청구권’을 보다 엄격한 형태로 구체화 한 것입니다. 특히 민간 영역에서 정보통신망을 통하여 주민등록번호가 수집, 보관되어 이용되는 경우 해당 정보가 유출되어 주민등록번호의 도입 목적 외로 활용될 가능성이 커지므로 주민등록번호에 대한 정보통신망을 이용한 수집제한청구권의 보호가치는 더욱 크다고 할 것입니다.

요컨대 개인정보보호법 제24조 및 정보통신망법 제23조의2 제1항 본문은 개인정보자기결정권이라는 기본권에서 도출되는 주민등록번호의 "행정목적 외 민간사용 금지" 원칙을 확인적으로 기술한 것입니다. 즉 정보통신망법 제23조의2 제1항은 법령의 형식을 띠고 있지만 결국 개인정보자기결정권에서 도출되는 헌법상 원리를 구체적으로 기술한 성격을 가진다고 할 것입니다.

라. 고유식별번호의 민간 활용을 금지시키거나 엄격히 제한하는 해외 사례

해외의 경우에도 복지, 세금부과 등 행정적 목적에 의해 국민에게 복수의 고유식별번호를 부과하고 있고, 해당 고유식별번호의 도입 취지와 어긋나는 민간 부문의 활용을 법령으로 금지하거나 엄격하게 제한하고 있습니다.

(1) 캐나다

캐나다의 경우 우리나라와 같은 주민등록번호 제도를 가지고 있지 않은 대신 사회보험번호 (SIN : Social Insurance Number)를 사용하고 있습니다. 사회보험번호는 주민등록번호와는 달리 그 용도가 엄격하게 제한되어 있는데, 벌금부과, 소득세징수, 실업급여 등 15개 행정업무에만 사용할 수 있도록 되어 있으며, 법률의 규정이 없는 한 사회보험번호의 수집 등의 행위가 프라이버시침해를 상회하는 사회적 이득이 있음이 규정된 경우에만 사회보장번호의 수집·사용이 가능하고, 사회보험번호의 제시를 요구하는 경우 개인에게 제시요구의 목적과 강제성 여부, 제시 거부 시의 결과에 대하여 미리 고지하여야 합니다.

(2) 스웨덴

스웨덴의 표준통일식별번호는 현재 조세·사회보장·병무행정 등에 광범위하게 사용되고 있습니다. 다만 스웨덴의 경우 우리와는 달리 거의 완벽한 사회보장체계를 갖추고 있는 나라로서, 사회보장제도를 비롯한 국가의 행정작용에 사용되는 개인식별번호는 국민의 편의와 생활안정에 직접적인 역할을 하고 있고, 이러한 점에서 주로 감시와 통제를 위해 사용되는 우리나라의 주민등록번호와는 근본적인 차이를 보이고 있습니다.

스웨덴 개인정보보호법(Personal Data Act 1998 : 204)은 명문의 규정으로 ‘민감한 개인 정보(sensitive personal data)’를 밝히고 구체적으로 인종, 민족적 배경, 정치적 견해, 종교적, 철학적 신념, 노동조합 회원의 신분 및 건강, 성생활과 관련된 개인 정보의 처리를 금지하고 있습니다.

같은 법 제22조는 처리 목적, 신원 보안의 중요성, 기타 중요한 사유가 명확한 경우를 제외하고는 본인의 동의 없이 개인식별번호를 사용할 수 없도록 규정하고 있습니다. 한편 같은 법 제50조의 규정을 통하여 정부 또는 정부가 지명한 기관으로 하여금 개인식별번호를 사용할 수 있는 범위를 특정하도록 하고 있으며, 본 법에 따른 감독 당국의 결정은 규정에 관련된 경우가 아니라면 일반행정법원에 항소할 수 있습니다.

(3) 독일

독일 신분증법의 경우, 일련번호에는 인적사항이나 기타 사항의 내용을 담을 수 없고(5조 8항), 10년마다 신분증 재발급하고 연장되지 않으며(6조, 따라서 번호 재발행), 신분의 전자적 증명 외에는 신분증을 개인정보의 자동저장, 개인정보의 자동검색에 사용할 수 없고(20조 2항), 일련번호를 데이터베이스로부터 개인정보를 추출하거나 데이터베이스의 연결을 가능하게 하는데 사용할 수 없으며(20조 3항), 20조 2항, 3항을 위반한 행위에 대해서는 벌금에 의해 처벌됩니다(32조).

참고로 독일은 1986년 제정의 신분증법에 따라 국민신분증제도를 도입할 때 이미 위와 같은 금지사항을 두고 있었고, 2009년 신분증을 전자카드로 만들면서 '신분증 및 전자적 증명법'으로 개정한 이후에도, 여전히 위 금지사항을 유지하고, 신분증을 '신분의 증명' 목적으로만 사용하도록 하는 구조를 유지하고 있습니다.

(4) 호주

호주의 경우 각 행정기관이 필요에 의해 사용하는 조세과일번호(Tax File Number, TFN), 의료보험증번호(Medicare card number) 등이 있으나 용도가 매우 제한적이며 신분확인용으로는 사용되지 않고 있는 실정입니다. 즉 호주에서는 주민등록번호와 같은 전국민적 개인식별번호는 존재하지 않습니다. 다만 호주에서도 우리나라의 주민등록증과 같은 국가신분증 도입을 위한 논의가 수 차례 있었습니다. 첫 번째는 1980년대 노동당 정부(Labor Government)가 제안한 “오스트레일리아 카드(the Australia Card)” 제도인데, 주민등록증과 유사하게 만 18세 이상의 호주 국민이라면 무조건 동 카드를 발급 받아야 하고, 카드발급 시 개개인에게 주민등록번호와 같은 고유한 카드번호가 부여되며, 신원증명, 사회보험의 목적뿐만 아니라 계좌개설, 부동산 매매 등 모든 금융거래 시 카드번호를 제공해야 했습니다. 하지만 상원 및 야당에서 반대했을 뿐만 아니라, 엄청난 국민적 반대에 부딪혀 결국 법안은 통과되지 못했습니다. 이후 2005년 런던 폭탄 테러 사건을 계기로 2005년과 2006년에 범죄와 테러의 방지를 위한 목적을 내세운 신분증 도입 논의가 재개되었지만 실현되지 못하였으며, 마지막으로 2006년에 연합정당이 사회보장제도 등의 이용을 위한 액세스 카드(the Access Card) 도입 법안을 제안했지만 이 역시 2007년 폐기되었습니다.

결론적으로 호주에서는 오스트레일리아 카드 법안을 계기로, 우리나라의 주민등록증과 같은 국가적 신분증 제도나 전 국민에게 개인식별번호를 부여하는 제도는 전체주의 국가로 나아가는 국가적 감시의 초석이 되고, 프라이버시에 대한 중대

한 침해이며 기능의 확장(function creep: the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, esp. when this leads to potential invasion of privacy)의 위험이 있으므로 절대 받아들일 수 없다는 국민적 공감대가 형성되어 있습니다. 따라서 우리나라의 주민등록번호와 같은 개인식별자를 부여하는 신분증 제도는 호주에서는 상상도 할 수 없는 전체주의적 시도라고 할 것입니다.

(5) 일본

일본 주민기본대장법(住民基本台帳法)상의 주민표 코드는 활용 가능 분야를 이른바 Positive 방식으로 규정하여 공공분야에서 제한된 부분에서만 활용 가능하였습니다. 이 외에도 기초 연금 번호, 건강 보험 피보험자 번호, 여권 번호, 납세자 번호, 운전 면허증 번호, 주민 표 코드, 고용 보험 피보험자 번호 등 각 행정기관이 개별적으로 번호를 부여하여 국민의 개인 정보 관리가 일괄적으로 이루어지지 않았는데, 즉 한 사람 당 한 개의 개인식별번호로 모든 행정 서비스를 포괄하는 제도는 시행하지 않았던 것입니다. 그러나 2013. 5. 31. “행정절차에 있어서 특정개인을 식별할 수 있는 번호의 이용 등에 관한 법률”(이른바 ‘마이넘버법’)이 제정되었고 2016년 시행을 앞두고 있습니다. 해당 법률은 우리나라의 주민등록번호와 같이 국민이나 법인에 식별번호를 부여하는 것을 내용으로 하고 있습니다.

그러나 이 법률은 해당 식별번호를 활용할 수 있는 주체를 “행정 기관, 지방 자치 단체 기타 행정 사무를 처리하는 자”로 명확히 해두고 있고 입법 목적 역시 “행정 운영의 효율화 및 행정 분야에서보다 공정한 급부와 부담의 확보”라고 명시하고 있으며, 민간분야의 사용은 시행 3년 후 검토를 거쳐 결정하는 것을 내용으로 하고 있어 원칙적으로 고유식별번호의 민간 활용금지 원칙이 포함되어 있습니다.

마. 소결

모든 국민에게 강제적으로 부여되는 개인식별번호인 주민등록번호에 대해서 도입 목적인 행정 목적 외에 민간에서 사용되어서는 안된다는 원칙은 개인정보자기결정권을 구체화한 것으로, 정보통신망법 제23조의2 제1항 본문에 규정되어 있습니다. 이는 이른바 고유식별번호의 기능의 확장(function creep)이 개인정보자기결정권을 침해할 여지가 매우 크다는 점을 보여주고 있으며 해외 입법 사례에서도 고유식별번호의 행정목적 외 민간사용 금지 원칙을 확인할 수 있습니다.

V. 이 사건 법조항의 개인정보자기결정권 침해

1. 이 사건 법조항의 개인정보자기결정권 제한

이 사건 법조항은 아래와 같습니다.

정보통신망법 제23조의2(주민등록번호의 사용 제한)

① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우

이 사건 법조항은 본인확인기관의 개인정보자기결정권의 보호대상이 되는 주민등록번호의 수집, 이용 행위에 대한 것이므로 원칙적으로 개인정보자기결정권에 대

한 제한에 해당합니다. 이 사건 법조항은 개인정보보호법 제24조와 정보통신망법 제23조의2 제1항 본문으로 보호하고 있는 개인정보자기결정권을 제한하고 있다는 점은 명백하다고 할 것입니다.

특히, 헌법재판소는 이와 같이 사람의 신원을 식별하는 정보 즉 본인확인 정보의 수집, 보관을 의무화하는 인터넷 실명제에 대해 다음과 같이 판시한 바 있습니다. (헌법재판소 2012. 8. 23. 자 2010헌마47 결정)

“본인확인제는 정보통신서비스 제공자에게 게시판 이용자의 본인확인정보를 수집하여 보관할 의무를 지우고 있는데, 본인확인정보는 개인의 동일성을 식별할 수 있게 하는 정보로서 개인정보자기결정권의 보호대상이 되는 개인정보에 해당하고, 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.(헌재 2010. 5. 27. 2008헌마 663, 판례집 22-1하, 323, 333 참조).”

문언적으로 보면 이 사건 법조항은 본인확인기관으로 지정된 정보통신서비스제공자들을 수집금지 의무에서 해방하는 것처럼 읽히지만, 전체 법체계에서 살펴보면 이 사건 법조항은 인터넷 실명제와 마찬가지로 본인확인기관에게 본인확인정보인 주민등록번호의 수집, 보관의무를 부여하고 있다고 보아야 하며, 개인정보자기결정권의 제한에 해당함은 당연하다고 하겠습니다

2. 주민등록번호 강제 부여의 위헌성

이 사건 법조항은 본인확인기관에 주민등록번호를 수집 이용을 의무화하고 있는데, 본격적인 위헌론을 펼치기 전에 주민등록번호 제도 및 본인확인기관 지정행

위의 위헌성을 따져봄으로써 수집제한의 필요성을 강조하고자 합니다.

주민등록 제도는 다음과 같은 이유로 침해의 최소성 원칙 및 법익의 균형성 원칙을 위반하는 등 헌법 제37조 제2항의 과잉금지의 원칙을 위반하여 위헌입니다.

침해의 최소성에 대해 헌법재판소는 “입법자는 공익실현을 위하여 기본권을 제한하는 경우에도 입법목적 실현하기에 적합한 여러 수단 중에서 되도록 국민의 기본권을 가장 존중하고 기본권을 최소로 침해하는 수단을 선택해야 한다.”고 선언하였는 바(헌재 1998. 5. 28. 96헌가5), 주민등록번호제도는 인구의 동태를 상시로 명확히 파악하여 주민생활의 편익을 증진시키고 행정사무의 적정한 처리를 도모한다는 주민등록법의 입법 목적을 달성하기 위한 필요 최소한의 수단이 아닙니다.

즉, 개인의 성명, 생년월일, 주소 정보만으로도 인구의 동태 파악을 위한 개인식별은 얼마든지 가능하고, 실령 개인을 식별하기 위한 번호를 부여하는 것이 불가피하더라도 각각의 행정영역마다 개인에게 별도의 식별번호를 활용하는 방법이 있을 수 있음에도 불구하고(헌재 운전면허번호, 의료보험번호, 여권번호, 예금계좌번호, 신용카드번호, 학번, 군번 등), 그 사람의 나이, 생년월일, 성별, 지역 등을 한번에 알 수 있게 하는 13자리 숫자코드로 구성된 주민등록번호제도는 국민의 개인정보자기결정권을 침해합니다.

주민등록번호제도로 인하여 보호하려는 공익은 주민의 거주관계 파악, 주민생활의 편익 증진, 행정사무의 적정한 처리인데, 이러한 공익을 달성하기 위하여 법령에 의해 시행되고 있는 13자리 숫자의 개인식별용 주민등록번호 제도는 지나치게 많은 개인의 정보를 하나의 숫자 체계에 담고 있다는 점, 이로써 국민에 대한 감시와 통제의 수단으로 작용하여 국민의 자유로운 사생활의 영역이나 인격의 발현에 위축을 받지 않을 수 없다는 점, 나아가서 공공영역은 물론 민간영역에서까

지 주민등록번호가 수집 및 활용되고 있고 주민등록번호 유출로 인한 피해가 심각한 수준인 점을 고려한다면 주민등록번호 제도는 그 법익의 균형성을 상실한 것입니다.

이상과 같은 주민등록번호제도는 위에서 언급하였듯이 민간부분이 자유롭게 수집하게 된다면 위의 위헌성이 전혀 완화되지 않을 것입니다. 그런데 이미 866개의 법령이 수집을 허용하거나 요구하고 있습니다⁴. 헌법재판소는 이 모든 법령들의 개인정보자기결정권의 침해여부를 판단해야겠지만, 청구인은 그 중에서 이 사건 법조항이야말로 아래의 판단기준에 비추어볼 때 가장 위헌성이 높은 조항이라고 판단하여 이 사건 청구에 이르게 된 것입니다.

3. 개인정보자기결정권 침해의 판단 기준

자신에 관한 개인정보가 언제 어떻게 그리고 어느 범위까지 타인에게 전달되고 이용될 수 있는지를 정보주체가 자율적으로 결정할 수 있는 권리인 개인정보자기통제권이 헌법에 의해 부여된 권리라는 점에 이론은 없습니다. 따라서 개인정보자기결정권은 법률이 아닌 헌법적 원리에서 조망되어야 함은 이미 앞서 밝힌 바와 같습니다.

즉 이 사건 법조항은 주민등록번호에 대하여 정보통신서비스 제공자 중 본인확인기관에게만 이를 수집, 보관, 유통을 담당하게 하고 있다는 점에서 민간영역인 본인확인 기관에 의한 주민등록번호 수집 이용 허용이 국민의 개인정보자기결정권을 본질적으로 침해하는지 여부를 엄격하게 심사해야 할 것입니다.

(1) 개인정보자기결정권 제한의 한계

⁴ <주민등록번호 수집 금지 제도 가이드라인> 안전행정부 개인정보보호과 (2014. 1.)

헌법상 개인정보자기결정권이 개인정보에 대한 실질적인 보호를 통해 프라이버시 권리 및 인간의 존엄성을 보장하기 위한 가치를 갖는 권리이기는 하나 정보주체는 누구나 우월적인 이익(공익)을 위하여 개인정보자기결정권에 대한 제한을 감수해야 하며, 개인정보자기결정권도 다른 기본권과 마찬가지로 헌법 제37조 제2항에 의하여 국가안전보장·질서유지·공공복리를 위하여 불가피한 경우에는 제한을 받게 됩니다.

다만, 그 제한은 법률에 의하되, 그 조건·범위·제한의 내용 등이 명확하게 그리고 한정적으로 규정되어야 하며, 과잉금지의 원칙을 준수해야 합니다. 즉, 개인정보자기결정권은 제한 목적이 정당하고, 그 수단이 적합해야 하며, 그 목적과 수단 사이를 비교 형량하여 제한여부를 판단하되, 제한하는 경우에도 최소한에 그쳐야 하는 것입니다.

(2) 개인정보자기결정권 제한의 정당화 기준

사회 공동체의 이익 또는 공익이 개인정보자기결정권의 제한을 언제나 정당화하는 것은 아닙니다. 중요한 것은 기본권의 본질로부터 도출되는 개인정보자기결정권의 제한가능성이 아니라 개인정보 자기결정권에 대한 제한이 어떠한 요건에서 허용되며 이에 관한 규정은 어떻게 형성되어 있어야 하는가 하는 점입니다. 우선 개인정보자기결정권에 대한 제한은 법률의 근거를 필요로 하며 당해 법률상의 제한의 요건과 범위는 명확하여 국민이 인식할 수 있고 따라서 규범명확성의 법치국가적 원칙을 충족하여야 하며, 또한 입법자는 이를 규율함에 있어 과잉금지의 원칙을 준수하여야 합니다.⁵

⁵ BVerfGE 65, 1 (44).

가. 명확성의 원칙

공권력에 의하여 이루어지는 개인정보의 조사, 저장, 제공, 공개 등은 개인정보 기결정권이라는 기본권의 제한이라 할 수 있으므로, 그 제한에는 반드시 법률의 수권이 있어야 합니다. 개인정보의 처리를 허용하는 법률이 있다고 하더라도 그것은 법치국가원리에서 도출되는 명확성의 요청을 따라야 하는데, 규범의 의미 내용으로부터 무엇이 금지 되는 행위이고 무엇이 허용되는 행위인지를 수범자가 알 수 없다면 법적 안정성과 예측 가능성은 확보될 수 없게 될 것이고, 또한 법 집행당국에 의한 자의적 집행을 가능하게 할 것이기 때문입니다.⁶

특히 개인정보의 수집·처리와 관련지어 보면 이러한 규범명확성(Normenklarheit)의 원칙은 자신에 관한 정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 해당 개인이 명확하게 인식할 수 있어야만 한다는 것을 뜻합니다. 여기서 의도된 데이터 처리의 목표는 물론 그 범위의 영역별로 법률에 명확하게 규정되어야 합니다. 따라서 조직적이고 절차법적인 예방책들, 관할기관들의 통지의무, 관련자의 포괄적인 설명청구권 등에 관한 법률의 명시적인 언급을 통하여 누가, 언제, 어디에서 어떤 경우에 자기의 개인정보에 접근할 수 있는지를 해당 정보 주체가 알 수 있도록 보장되어야 합니다.

특히 관련자가 법규정으로부터 그의 개인 관련정보가 어떤 구체적인 행정목적을 위하여 필요한지를 명백히 인식할 수 있어야만 합니다. 하지만 입법자가 각 개인의 법률상 의무에 대하여 구체적 목적까지 그 법률에서 밝힐 필요는 없고, 일반적으로 그 목적이 당해 법률의 체계 및 입법 취지 등에 비추어 그 의미가 분명하

⁶ 헌법재판소 1990. 4. 2. 89헌가113, 판례집 2, 49면 참조.

여 질 수 있다면 그 법률은 이미 충분히 명확하다고 할 수 있습니다.⁷

나. 목적구속성의 원칙

이와 관련하여 개인정보자기결정권을 제한하는 입법의 체계는 정보처리의 각 영역별로 특수하게 규율하는 형태를 취하여야 한다는 요청이 나타납니다.⁸

즉, 개인정보의 수집은 법률에 의하여 특정된 목적범위 내에서만 허용되어야 하며, 이때의 목적은 규범명확성의 원칙에 따라 일반인이 당해 법률로부터 자신의 개인정보가 왜 필요한 것인지 분명하게 알 수 있을 정도로 특정된 것이어야 합니다. 또한 목적은 정보수집이 목적달성에 적합한 것인지 그리고 필요한 최소한의 것인지를 여부를 판단하는 것이 가능하도록 구체적으로 규정되어야 합니다.⁹

따라서 불특정한 목적 또는 아직 확정할 수 없는 목적을 위해 개인정보를 미리 수집하는 것은 목적구속의 원칙에 반합니다. 그러나 정보의 저장은 그 개념상 장래의 사용을 위하여 준비해 놓는다는 의미가 내포되어 있으므로 미리 정보를 수집하는 것 자체가 금지되는 것은 아니며, 단지 사용목적이 명확히 확정되어 있지 않다는 점이 문제되는 것이므로 법률에 의하여 사용목적이 구체적으로 특정되고 정보의 사용이 그에 한정된다면 장래의 목적을 위한 정보의 저장도 허용될 수 있다고 할 수 있습니다.¹⁰

⁷ BVerfGE 65, 1 (54).

⁸ BVerfGE 65, 1 (44, 46)

⁹ BVerfGE 65, 1 (53).

¹⁰ Franz-Ludwig Knermeyer, Datenerhebung und Datenverarbeitung im Polizeirecht, NVwZ 1988, S. 194.

법률에 규정된 특정한 목적을 위해서 수집된 정보는 그 목적을 위해서만 저장되고 이용되어야 합니다. 목적구속성의 원칙에 따라 경우 특정한 목적을 위해 수집된 정보가 다른 허용되지 않은 목적을 위해 저장·변경 또는 이용되어서는 안되며, 정보수집목적의 변경은 새로운 개인 정보자기결정권에 대한 침해가 될 수 있기 때문에 입법자는 그 요건을 법률로서 규율하여야 하며 따라서 정보수집목적의 변경은 법률에 규정된 특별한 요건 하에서만 제한적으로 인정될 수 있을 뿐입니다.¹¹

다. 과잉금지의 원칙¹²

개인정보자기결정권도 헌법상 인정될 수 있는 기본권인 만큼, 그 제한에 있어서 기본권 제한의 일반원칙인 과잉금지원칙이 준수되어야 함은 당연합니다. 다만 과잉금지의 원칙상 정보의 중요도에 따라 그 제한의 정도가 달라질 수는 있을 것입니다.

물론 독일의 연방헌법재판소가 인구조사 판결에서 밝힌 바와 같이 정보의 전산처리라는 현대적 상황 하에서 중요하지 않은 정보란 사실상 존재하지 않는다고 하였고, 오늘날 개인정보가 다른 정보와 결합 내지 연동되는 측면에서 타당한 면도 있지만, 사상이나 전과사실, 병력(病歷) 등과 같이 그 자체로서 내밀한 영역을 드러내는 민감한 개인정보인 경우에는 그 수집 내지 보유만으로도 기본권 침해의 가능성이 크기 때문에 특별히 강화된 보호가 필요할 것입니다. 이러한 점에서 개인정보자기결정권과 관련된 과잉금지원칙의 일반적 내용은 다음과 같습니다.

¹¹ Helmut Bäumler, Informationsverarbeitung im Polizei- und Strafverfahrensrecht, in: Liskén / Denninger, Handbuch des Polizeirechts, 3. Aufl., 2001, Rn. 35.

¹² <개인정보자기결정권의 제한과 전자여권>, 이상명, 법학논총, 한양대학교 법학연구소 (2008) pp.164-166

첫째, 개인정보자기결정권을 제한하려는 목적이 정당하여야 합니다.

즉 정보주체의 동의를 얻지 아니하고 개인정보를 취급하는 경우 그것이 법률의 규정에 의한 것이라 하더라도 각 단계별로 달성하고자 하는 목적이 정당하여야 한다는 것입니다. 가령 정보주체의 동의에 의하지 않은 개인정보의 수집이나 열람거부, 목적 외 이용, 대외적 공표 등이 국가안전보장, 질서유지 또는 공공복리를 위해서 이루어지거나 허용되는 경우 그 목적의 정당성이 인정될 수 있습니다.

둘째, 개인정보자기결정권을 제한하는 조치가 목적을 달성하는 데 적합한 수단이어야 합니다.

따라서 개인정보의 수집과 처리는 추구하는 목적을 달성을 하는 데 효과적인 수단일 것이 요구됩니다. 그러나 만일 개인정보의 비밀수집이나 공개 등의 조치를 취하더라도 해당 목적을 달성하는 데는 별다른 효과를 기대하기 어려운 경우라면 수단의 적합성은 인정될 수 없습니다.

셋째, 해당 목적을 위한 경우라도 필요최소한의 정보처리가 요구됩니다.

공권력에 의한 개인정보의 처리는 명백하고 정당한 공적 과제의 이행이라는 목적에 기여하는 경우라 하더라도 이러한 목적을 달성하는 데 있어서 적합한 방식으로 필요한 최소한으로 이루어져야 합니다. 가령 행정기관간의 정보공유가 필요한 경우라 하더라도 그 개인정보를 보유하고 있는 기관은 그 개인정보가 무한히 전달되거나 이용되는 것을 막는 조치를 취하여야 할 것이며, 이를 위하여 행정기관은 보유하고 있는 개인정보를 다른 관청의 과제로부터 분리시킬 필요가 있는 것입니다.

더욱이 주민등록번호와 같이 민간 영역에서 수집, 이용하는 행위 자체가 개인정보자기결정권 침해를 구성할 가능성이 큰 경우 공권력에 의한 개인정보의 처리에 비해 정당한 공적과제의 이행이라는 목적에 기여하는지 여부가 엄격하게 판단되어야 하며, 주민등록번호의 민간 영역 활용이 목적 달성에 있어서 필요 최소한으로 이루어지는지에 대해서 역시 더욱 엄격하게 판단되어야 할 것입니다.

넷째, 개인정보자기결정권의 제한이 불가피하고 최소한으로 이루어지는 경우라 하더라도 법익의 균형성이 요청됩니다.

즉 개인정보자기결정권의 제한으로 인한 피해의 이익이 그 제한을 통하여 달성하고자 하는 공익보다 적어야만 정당한 기본권제한이 될 수 있는바, 보호이익과 피해이익 사이의 형량에 있어서는 개인정보에 대한 침해의 성질, 강도, 민감성 등이 고려되어야 합니다.

2. 이 사건 법조항의 개인정보자기결정권 침해

이 사건 법조항은 아래와 같이 명확성 원칙, 목적구속성원칙 및 헌법 제37조 제2항의 과잉금지원칙을 위반하여 청구인의 개인정보자기결정권을 침해하고 있습니다.

(1) 명확성 원칙 위반

개인정보자기결정권과 관련한 명확성(Normenklarheit)의 원칙은 자신에 관한 개

인정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 해당 개인이 명확하게 인식할 수 있어야만 한다는 원칙입니다.

주민등록번호와 같이 키 데이터(key data)에 해당하는 개인정보인 경우에는 해당 정보의 수집 내지 보유만으로도 기본권 침해의 가능성이 크기 때문에 명확성의 원칙에 비추어 특별히 강화된 보호가 필요합니다. 주민등록번호의 수집, 이용을 규율하기 위해서는 주민등록번호 사용과 관련하여 본인확인기관에 대한 조직적이고 절차법적인 예방책들, 관할기관들의 통지의무, 관련자의 포괄적인 설명청구권 등에 관한 법률의 명시적인 언급을 통하여 누가, 언제, 어디에서 어떤 경우에 자기의 개인정보에 접근할 수 있는지를 해당 정보 주체가 알 수 있는지가 사전에 명확하게 규율되어야 하는 것입니다.

그러나 주민등록번호의 민간 영역에서의 수집, 이용 자체만으로도 개인정보자기 결정권 침해의 여지가 큼에도 불구하고 이 사건 법조항에는 본인확인기관이 어떠한 처리목적을 위하여 주민등록번호를 수집, 이용하도록 허용하고 있는지가 불분명합니다. 정보통신망법은 본인확인기관의 목적을 ‘대체수단’의 개발, 제공, 관리라는 점만을 규율하고 있을 뿐, 달리 어떠한 구체적 처리목적들을 위해 주민등록번호가 수집되는지, 어떠한 과정을 거쳐 주민등록번호가 활용되는지, 누가 수집된 주민등록번호에 접근할 수 있는지에 대해 전혀 기술하고 있지 않습니다.

따라서 이 사건 법조항에 의하여 민간 영역인 본인확인기관에 의해 수집된 주민등록번호가 어떠한 처리목적들을 위해 사용되는지에 대해서는 입법취지나 관련 법조항에서도 전혀 예측할 수 없기 때문에 개인정보자기결정권에 요구되는 명확성 원칙에 위배됩니다.

(2) 목적구속성 원칙 위반

명확성의 원칙에 따라 일반인이 당해 법률로부터 자신의 개인정보가 왜 필요한 것인지 분명하게 알 수 있을 정도로 특정된 것이어야 하며, 또한 이러한 목적은 정보수집이 목적달성에 적합한 것인지 그리고 필요한 최소한의 것인지를 여부를 판단하는 것이 가능하도록 구체적으로 규정되어야 합니다.

그러나 앞서 살펴본 바와 같이 이 사건 법조항은 본인확인기관이 주민등록번호를 수집, 이용하는 것을 내용으로 하는 처리 목적을 명확하게 밝히지 않았으며, 따라서 민간 영역에 있는 본인확인기관이 주민등록번호를 수집 이용하는 것이 해당 목적 달성을 위해 필요한 최소한의 것인지 여부를 판단할 수 없어 목적구속성 원칙에 위배됩니다.

결국 이 사건 법조항이 본인확인기관으로 하여금 주민등록번호를 수집하도록 하는 것은 불특정한 목적 또는 아직 확정할 수 없는 목적을 위해 개인정보를 미리 수집하는 것에 해당하여 목적구속성 원칙에 반합니다

(3) 헌법 제37조 제2항 과잉금지원칙 위반

가. 목적의 정당성

명확성 원칙 부분에서 살펴본 바와 같이 이 사건 법조항이 본인확인기관에게 주민등록번호를 수집할 수 있도록 한 목적 자체가 불분명하여 기본권 제한의 목적을 아래와 같이 유추해볼 수밖에 없습니다. 주지하다시피 정보통신망법 상 본인확인기관을 지정하는 목적은 주민등록번호를 사용하지 아니하고도 정보통신망서비스 회원으로 가입할 수 있는 방법(이하 “대체수단”이라 합니다)의 개발·제공·관리 업무를 위한 것입니다. 따라서 이 사건 법조항의 기본권 제한 목적은 대체수단의 개발, 제공 관리를 위한 것이라고 유추해볼 수 있습니다.

그러나 대체수단의 개발을 위해 민간에게 주민등록번호를 수집 이용하게 하는 것은 다음과 같은 이유로 정당한 목적이라고 보기 어렵습니다.

1) 대체수단의 개발이라는 목적은 주민등록번호 민간사용 금지원칙의 예외에 해당하지 않습니다.

그러나 ‘대체수단’의 개발은 개인정보자기결정권에서 도출되는 주민등록번호 민간사용금지 원칙의 예외가 될 수 없어 기본권 제한의 목적이 정당하다고 할 수 없습니다. 주민등록번호의 도입 및 사용 목적은 주지하다시피 주민의 거주관계 파악, 주민생활의 편의 증진, 행정사무의 적정한 처리인데 대체수단의 개발은 이와는 무관합니다. 정보통신망법상 ‘대체수단’은 행정 영역이 아닌 민간 영역에서 정보통신망 서비스를 이용하기 위해 요구되는 ‘회원가입’ 과정에서 본인확인 목적으로 이용되는 수단에 불과하기 때문입니다.

2) 이 사건 범조항은 개인정보자기결정권을 보장해야 하는 국가가 입법을 통하여 국민들의 개인정보를 민간 영역의 사업자들에게 보유하게 하고, 국민의 개인정보를 이용한 개인정보 사업을 합법화 시켜주고 있습니다.

청구인의 주민등록번호를 유출한 주식회사 케이티의 경우 다른 정보통신서비스 제공자들에게 본인확인기관으로서 대체수단 서비스를 제공하는 사업을 영위하고 있습니다. 이는 국민의 개인정보자기결정권을 보장해야 하는 국가가 가장 보호가치가 큰 개인정보 중 하나인 주민등록번호를 민간 사업자에게 확보할 수 있도록 하고 이를 활용하여 사업을 하도록 권한을 주는 것으로서 정당한 입법목적이라고

할 수 없습니다.¹³

3) 소결

따라서 이 사건 법조항은 단지 대체수단 개발의 용이성을 담보하기 위하여 본인 확인기관에게 이용자들의 주민등록번호를 수집, 이용하도록 하고 있으므로 기본권 제한 목적의 정당성 자체가 인정되지 않는다고 할 것입니다.

나. 방법의 적정성

이미 정보통신서비스 제공자를 대상으로 한 여러 번의 대규모 유출사건을 통하여 국민의 주민등록번호가 대규모로 유출되었고 정보통신망을 통해 유통되고 있기 때문에 주민등록번호를 기반으로 하거나 이를 활용한 대체수단의 개발은 입법목적 달성에 전혀 효과적인 방법이 아닙니다. 따라서 대체수단 개발을 위해 본인확인기관이 주민등록번호를 수집, 사용하도록 하는 이 사건 법조항은 방법의 적정성 요건을 충족하지 않습니다.

본인확인기관으로 지정된 이동통신사의 경우 회원 가입 시 가입자의 이름과 주민등록번호의 조합이 유효한 지를 확인하여 이를 통하여 본인임이 확인되면 해당 가입자에게 부여한 이동통신 전화번호를 소유한 자가 주민등록번호 상 실지 명의 자임을 확인해주는 방식으로 대체수단을 제공하고 있습니다.

그러나 정보통신망법 상 대체수단은 ‘주민등록번호’를 사용하지 않는 본인확인 수단임에도 불구하고 본인확인기관으로 하여금 주민등록번호를 활용하여 대체수단

¹³ <온라인상 주민등록번호 수집금지 정책의 시행과 쟁점>, 심우민, 국회입법조사처, 이슈와 논점 제614호 (2013. 3. 4.)

을 개발할 수 있도록 한다면 이를 통해 개발, 운용되는 수단은 앞으로도 영원히 주민등록번호를 사용해야만 유지될 수 있습니다. 즉, 이 사건 범조항이 본인확인 기관으로 하여금 주민등록번호를 사용하지 않는 대체수단의 도입이라는 목적 달성에 전혀 기여하지 못합니다.

이러한 점은 이번 본인확인기관 해킹 사건을 통해 명백히 드러난 바 있습니다. 주식회사 케이티는 청구인과 같은 이용자들에게 해킹 사건으로 주민등록번호가 유출되었는지 여부를 공지할 때에 본인확인 목적을 위해 재차 주민등록번호를 요구했습니다.¹⁴ 결국 이를 통해 본인확인기관이 스스로 개발하여 운용하고 있는 대체수단은 주민등록번호를 그대로 이용하고 있다는 점을 자인하고 있다고 할 것입니다. 이 사건 범조항이 본인확인기관에게 주민등록번호를 수집, 이용하도록 하는 것이 대체수단 개발이라는 목적 달성에 전혀 기여하지 않으며, 오히려 목적 달성을 적극적으로 방해하고 있는 것입니다.

또한 이미 주민등록번호가 대규모로 유출된 이상 주민등록번호를 도용하여 실지 명의자가 아님에도 대체수단을 발급받을 가능성(identity theft)이 매우 크므로 주민등록번호를 활용하거나 주민등록번호를 담보로 하여 개발되어 운영되는 대체수단은 정보통신망법이 대체수단을 도입하려는 입법목적 달성에 전혀 효과적이지 않습니다. 정보통신서비스 제공자에 의해 주민등록번호가 유출되더라도 유출된 피해자가 주민등록번호를 정정할 수 있다면 주민등록번호를 활용한 대체수단이 입법목적 달성에 효과가 있을 것입니다. 그러나 현재 행정청 및 법원은 개인정보가 유출된 경우를 주민등록번호 정정 사유로 인정하고 있지 않습니다. 따라서 이미 대규모로 유출된 주민등록번호를 그대로 사용하는 방식의 대체수단은 유출된 주민등록번호를 활용한 부정사용(identity theft)의 가능성에서 자유로울 수 없어 이 사건 범조항은 방법의 적정성을 충족하지 못합니다.

¹⁴ kt 개인정보 유출확인, 주민등록번호 또 입력하라는 안내에 네티즌들 "폭발", 조선일보 (2014. 3. 11.)

다. 피해의 최소화

비례성 판단 구조에 비추어 보면 방법의 적정성을 결여한 기본권 제한 조치는 피해의 최소화성이나 법익의 균형성을 따질 필요 없이 위헌이라고 판단되어야 마땅합니다. 그러나 방법의 적정성 문제에 관한 이견이 있더라도, 아래와 같이 다른 요건의 결여로 인하여 이 사건 법조항이 위헌적인 기본권 제한임을 밝히고자 합니다.

1) 대체수단의 개발, 제공, 관리 업무는 주민등록번호에 기반하지 않는 다른 수단에 의해서도 충분히 달성할 수 있습니다.

주민등록번호의 대체수단을 개발을 위해 본인확인기관에게 주민등록번호를 수집하도록 하면 이를 통해 개발된 대체수단은 주민등록번호를 완전히 대체할 수 있는 방법이라고 보기 어렵다는 점은 앞서 밝힌 바와 같습니다. 오히려 엄밀한 의미의 대체수단의 개발을 위해서는 본인확인기관 역시 주민등록번호 수집, 이용을 금지시켜야 하며 주민등록번호에 의존하지 않는 방식, 즉 덜 기본권 제한적인 방식으로 대체수단의 개발이 가능합니다.

① 정보통신망법 상 대체수단 개발을 위해서 필연적으로 신원정보를 표상하는 주민등록번호가 요구된다고 볼 수 없습니다.

정보통신망법 상 대체수단의 정의는 “주민등록번호를 사용하지 아니하고 본인을 확인하는 방법”입니다. 여기서 ‘본인확인’이란 최초에 정보통신서비스 이용을 위해 회원가입한 주체가 다시 해당 서비스를 이용하기 위해 접속하였을 때 그 주체

가 맞는지를 확인하는 것을 의미합니다. 이 사건 법조항이 예정하고 있는 대체수단이 수행하는 ‘본인확인’은 반드시 그 사람의 ‘신원정보’까지 확인하는 것을 요건으로 하고 있지 않는 것입니다.

그러나 주민등록번호를 활용한 본인을 확인하는 방식은 단순히 본인임을 확인하는 것을 넘어서는 것으로 ‘신원확인’이 더욱 적당한 표현일 것입니다. 주민등록번호에는 생년월일이나 출생지역 등 신원정보가 포함되어 있고, 주민등록번호를 키 데이터로 하여 다양한 신원정보들이 축적되어 있으므로 주민등록번호를 확인하는 방식은 ‘신원정보’를 확인하는 것에 해당합니다.

따라서 단순히 ‘본인임을 확인’하기 위해서 즉, 서비스를 이용하려고 하는 자가 회원가입을 했던 그 주체가 맞는지 알아내기 위해 그 사람의 신원정보까지 모두 파악할 필요는 없는 것입니다. 신원정보는 정보통신서비스 제공자가 서비스에 불가피하게 필요한 경우에 추가적으로 요구하면 될 것입니다. 그러나 대체수단의 개발, 운용을 위해 주민등록번호를 사용하는 순간 정보통신망법 상 대체수단은 ‘본인확인’을 넘어서 신원정보까지 확인하는 이른바 ‘신원확인’ 수단으로 기능하게 되는 것입니다.

② 주민등록번호 그 자체로 본인확인기관이 획득하는 신원정보는 반드시 주민등록번호를 통해서만 획득할 수 있는 것이 아니기 때문에 대체수단의 개발, 운용을 위해 반드시 주민등록번호가 요구되는 것은 아닙니다.

가사 대체수단을 개발하는데 반드시 이용자의 신원정보가 요구된다고 하더라도 반드시 주민등록번호를 활용해야 할 필요성은 없습니다.

주지하다시피 주민등록번호 앞 부분 6자리는 생년월일을 나타냅니다. 주민등록번호

호 뒷 부분 7자리는 성별, 지역과 검증번호로 구성되어 있습니다. 7자리 숫자를 abcdefg라고 할 때, a는 성별을, bcde는 지역코드(행정안전부장관이 부여하는 위시행규칙 제3조의 지역표시번호가 바로 bcde의 지역코드입니다), f는 그 날 등록지에서 출생신고를 한 순서대로 부여하며, 마지막 g는 검증코드로 일정한 수학적 규칙에 의해 부여됩니다. 결국 본인확인기관이 주민등록번호 그 자체를 통해 수집할 수 있는 정보는 생년월일이나 성별, 출생지 외에는 없습니다. 그 밖에 주민등록번호를 구성하고 있는 출생신고의 순서는 대체수단의 개발과는 무관하며, 수학적 규칙에 의한 검증코드 역시 주민등록번호 중복을 방지하기 위한 것이기 때문에 대체수단의 개발 그 자체와는 무관합니다.

따라서 대체수단 개발을 위해 본인확인기관이 정보주체의 생년월일이나 성별, 출생지와 같은 신원정보가 필요하다면 개인정보의 주체에게 ‘대체수단 개발’에 필요한 개인정보로 생년월일이나 성별, 출생지를 직접 요구하는 방식으로 해당 정보의 획득이 가능할 것이므로 주민등록번호 대체수단의 개발을 위해 그 전제로 반드시 주민등록번호가 요구되는 것은 아닙니다.

③ 주민등록번호 정보에 기반하지 않으면서도 정보통신서비스 제공에 필요한 범위의 정보로만 본인확인을 하는 수단이 존재합니다.

정보통신서비스 제공자들은 서비스의 성격에 따라 회원가입 시 본인확인을 하는 목적이 다양하고 이에 따라 대체적 본인확인 수단은 주민등록번호에 기반하지 않는 다양한 방식으로 개발 및 운용이 가능합니다.

가령 정보통신서비스 제공자가 회원과 금융 거래를 해야 한다면 주민등록번호가 아니라 회원의 ‘신용정보’나 ‘금융기관’과 관련된 정보를 활용하면 될 것입니다. 이 경우 이용자에게 이용자 명의로 가입한 신용카드 정보나 금융기관의 계좌 정

보를 등록하도록 하고, 해당 기관에 해당 정보가 정확한지를 확인하거나 매우 작은 금액으로 결제를 하도록 하고 실제로 이용자가 결제에 성공하는 경우 거래 능력이 있는 본인임을 확인하는 방식으로 본인확인이 가능합니다. 이 경우 주민등록번호를 사용하지 않으면서 정보통신서비스 제공에 필요한 한도에서 ‘본인확인’을 넘어서는 ‘신원확인’이 이루어진다고 할 수 있습니다.

한편 회원가입 시 신원정보가 요구되지 않는 예컨대 이메일 서비스와 같은 일반적인 정보통신서비스라면, 이용자가 회원 가입 시 지정한 아이디와 패스워드의 조합만으로 본인확인을 하도록 해도 무방합니다. 이 경우에 ‘신원확인’이 아닌 엄밀한 의미의 ‘본인확인’만으로도 정보통신서비스 제공이 가능하다고 할 것입니다. 만약 조금 더 엄격한 본인확인이 요구되는 경우 아이디와 패스워드 외에도 이용자가 별도의 질문과 대답을 정하도록 하고 정해진 질문에 대한 정확한 대답을 아는 자를 본인이라고 확인하는 방법도 존재합니다.

정보통신망법 상 본인확인기관의 임무는 이처럼 신원정보나 신원정보를 표상하는 주민등록번호에 의존하지 않고서도 본인 여부를 확인하는 다양한 수단을 개발하는 것에 있습니다.

결국 본인확인기관이라고 하더라도 반드시 신원정보를 표상하는 주민등록번호를 이용하여 대체수단을 개발해야 할 필요성은 없는 것이며, 주민등록번호를 이용하지 않는 덜 기본권 침해적인 본인확인 방식을 이용하여 대체수단을 개발, 운용해야 하는 것입니다. 오히려 주민등록번호를 이용한 방식은 대규모 유출사건으로 인하여 신원의 도용(identity theft) 문제로 본인확인의 정확성이 떨어질 가능성이 크다는 점은 앞서 살펴본 바와 같습니다.

2) 소결

따라서 정보통신망법 상 대체수단은 도입 취지에 맞게 주민등록번호를 기반하여 개발되어서는 안되며 주민등록번호를 활용하지 않는 본인확인 수단 즉, 덜 기본권제한적인 수단이 존재하므로, 주민등록번호를 대체하기 위해 다시 주민등록번호를 정보통신망을 통해 유통되게 하는 이 사건 법조항은 침해최소성 원칙을 충족하지 못합니다.

라. 법익의 균형성

개인정보자기결정권의 제한으로 인한 정보주체의 이익이 그 제한을 통하여 달성하고자 하는 공익보다 적어야만 정당한 기본권 제한으로 인정될 수 있는데, 다만 보호이익과 피해이익 사이의 형량에 있어서는 개인정보에 대한 침해의 성질, 강도, 민감성 등이 고려되어야 합니다.

이 사건 법조항은 민간부문에서 수집, 이용되는 것을 엄격하게 금지해야 할 성격의 ‘주민등록번호’를 민간부문인 본인확인기관에게 어떠한 활용 원칙의 제시도 없이 무제한적으로 수집 이용을 허용하고 있고, 더욱이 주민등록번호는 다른 개인정보와 결합되어 이른바 키 데이터(key data)로 활용되고 있는 매우 보호가치가 큰 성격의 것이므로 법익균형성의 비교형량이 더욱 엄격하게 판단되어야 할 것입니다.

1) 이 사건 법조항에 의해 개발, 운용되는 대체수단의 활용으로 인해 달성되는 공익은 불분명하고, 또한 주민등록번호를 계속 정보통신망에서 광범하게 유통되도록 하여 대체수단의 개발을 통한 정보통신망 상 주민등록번호 대체효과라는 공익을 전혀 달성하지 못합니다.

① 이 사건 법조항을 통해 개발된 대체수단을 이용한 본인확인의 목적이 불분명하

고, 다른 법령 상 주민등록번호 수집 권한 부여로 달성되는 공익과 비교하더라도 이 사건 법조항으로 달성되는 공익이 매우 적거나 불분명합니다.

우선 이 사건 법조항에 의해 본인확인기관이 개발 운용한 대체수단은 그 사용 목적이 불분명합니다.

이제까지 인터넷상 본인확인의 필요성을 대표해 왔던 제도는 게시판 이용자의 본인확인을 요구하는 ‘인터넷 실명제’였습니다. 그러나 2012년 헌법재판소는 민간영역 인터넷 게시판 실명제에 대해 위헌으로 결정한 바 있어 더 이상 인터넷 실명제를 위한 본인확인의 필요성은 존재하지 않습니다.

현재는 정보통신망법 상 공공 게시판 인터넷 실명제와 공직선거법 상 선거기간 중 게시판 실명제만 남아 있는 상황이나 인터넷 이용자들의 공공 게시판 활용빈도가 매우 낮은 상황이고, 선거기간 중 실명제 적용이 사실상 불가능한 사회관계망 서비스(Social Network Service, SNS) 서비스 활용이 비약적으로 증대되고 있습니다. 결국 실명제와 관련 하여 본인확인의 필요성이 매우 감소하고 있고 더욱이 이러한 인터넷 본인확인 규정들에 대해서는 헌법재판소의 결정에 비추어 전반적인 개선이 예견되고 있는 상황입니다. 따라서 제도적 차원에서 볼 때 본인확인의 수요는 매우 급감하고 있는 상황입니다.¹⁵

물론 유해 콘텐츠 및 게임 규제와 관련하여 청소년 보호를 목적으로 하는 성인인증 및 연령확인 업무에서 본인확인이 제도적으로 필요한 상황입니다. (청소년보호법 및 게임산업진흥법) 그러나 성인인증을 위해 연령확인을 넘어서는 본인확인까지 이루어져야 할 필연성은 존재하지 않으며, 이미 이러한 이유로 청소년보호법과 게임산업진흥법 상 본인확인제에 대해서 헌법소원이 제기되어 있는 상태입니다.

따라서 본인확인 제도가 급감하고 있음에도 이를 위해 다수의 민간영역 본인확인

¹⁵ <개인정보 유출사고와 본인확인기관 활용의 문제점>, 심우민, 국회입법조사처, 이슈와 논점 제 814호 (2014. 3. 17.)

기관을 제도적으로 활용해야 한다는 주장에는 문제가 있으며, 이는 본인확인 기관을 국가가 지정하여 그들에게만 독점적으로 주민등록번호를 사용할 수 있도록 권능을 부여함으로써 달성되는 공익이 거의 존재하지 않거나 불분명하다는 점을 방증하고 있습니다.

한편 정보통신망법 제23조의2 제1항 제2호에서 예정하고 있는 개별 법령에서 주민등록번호의 수집 및 이용을 허용하는 경우와 비교하면 이 사건 법조항으로 인하여 달성되는 공익이 거의 존재하지 않거나 불분명하다는 점을 비교해볼 수 있습니다. 다른 법령이 주민등록번호 수집을 허용하고 있는 주요 사례 및 수집 목적은 아래와 같습니다.

근거법령	내용
금융실명거래법 법§3, 령§3	금융거래시 성명· 주민등록번호 등으로 실지명의 확인
부가가치세법 법 §16, 령 §53	세금계산서상에 공급받는 자 의 주소·성명·주민등록번호 기재
부가가치세법 법 §72의2, 령 §63의2	세무서에 대손세액공제 신고 시 재화·용역을 공급받는 자 의 주민등록번호 기재
부가가치세법 법 §33, 령 §84	관할세무서에 납세관리인 선정 신고 시 납세관리인의 주민 등록번호 기재
소득세법 법 §145, 령 §193	기타소득 지급 시 원천 징수 영수증상에 주민등록번호 기재
소득세법 법 §164, 령 §213	기타소득 등에 대한 지급명세서 제출시 기타소득자의 주민 등록번호 기재

신용정보보호법 법 §34, 령 §29	신용정보회사는 신용정보 제공·이용자로부터 본인의 동의를 얻은 뒤 주민등록번호 등 개인정보 수집가능
전자서명법 법 §15, 규칙 §13의2	공인인증서 발급 시 발급자의 성명·주민등록번호 등으로 신원확인

출처 : <주민번호 사용 제한 정책 안내서> 방송통신위원회·한국인터넷진흥원, (2012. 6.), p. 4

② 이 사건 법조항은 정보통신망 상 주민등록번호 대체효과라는 공익을 달성하지 못합니다.

방법의 적정성 부문에서 이미 살펴본 바와 같이 본인확인기관이 대체수단을 개발, 운용하기 위해 다시 주민등록번호를 활용한다면, 결국 이를 통해 개발된 대체수단은 주민등록번호와 일대일로 대응(매칭)되는 성격의 것으로 사실상 주민등록번호가 정보통신망을 통해 계속 사용되도록 하는 성격의 것입니다. 즉 주민등록번호를 기반으로 개발된 수단은 주민등록번호를 겹으로만 대체하는 것일 뿐 사실상 주민등록번호를 그대로 표상하는 것이므로, 이하 이를 ‘유사 대체수단’이라고 지칭하겠습니다.

이미 정보통신망법 제23조의2 2항은 “(같은법) 제1항 제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.”고 정의하고 있으므로 정보통신망법 상 ‘대체수단’은 주민등록번호와 일대일로 대응되는 것이거나 주민등록번호를 기반으로 해서는 안된다는 점을 전제하고 있습니다.

정보통신망법 제23조의2

② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

결국 청구인과 같은 정보통신망 이용자는 정보 주체의 의사와는 무관하게 주민등록번호를 본인확인기관에게 제공해야 하며, 이 사건 법조항은 이른바 유사 대체수단 제공을 위하여 국민의 주민등록번호가 정보통신망을 통하여 계속 활용될 수 있도록 길을 열어준 셈입니다.

실제로 이동통신사가 본인확인기관으로 지정된 이후에도 청구인과 같은 이용자들은 본인확인기관이 제공하는 본인확인서비스를 이용하기 위해서는 정보통신망을 통해 주민등록번호를 계속 제공해야 합니다. 결국 이 사건 법조항은 회원가입 시 주민등록번호를 사용하지 않도록 하는 것을 목적으로 하고 있지만 오히려 본인확인기관으로 하여금 주민등록번호에 의존하도록 하고 있어 정보통신망 상 주민등록번호 대체효과가 전혀 발생하고 있지 않고 있는 것입니다.¹⁶

요컨대 이 사건 법조항은 정보통신망 상 주민등록번호가 계속 유통되도록 하고 있어 당초 목적인 공익 즉 대체수단의 개발을 통한 정보통신망 상 주민등록번호 대체효과를 실질적으로 달성하고 있다고 보기 어렵습니다.

¹⁶ "그러나 이러한 인증수단들도 최초 발급단계에 서는 주민등록번호 활용을 기본전제로 하고 있어 여전히 문제점을 가지고 있다. 따라서 우리나라의 주민등록번호는 향후에도 온라인상에서 상당한 가치를 유지할 것으로 예견된다. 물론 양적인 측면에서 주민등록번호의 활용이 감소한다고 볼 수도 있겠지만, 여전히 주민등록번호가 악용될 수 있는 구조라는 점에는 변함이 없다."

- <온라인상 주민등록번호 수집금지 정책의 시행과 쟁점>, 심우민, 국회입법조사처, 이슈와 논점 제614호 (2013. 3. 4.)

2) 반면 이 사건 법조항이 본인확인기관에 주민등록번호 수집 및 이용을 허용하는 것은 입법 목적 달성에 필요한 범위를 넘어서고 있어 청구인의 개인정보자기결정권의 제한은 매우 중대합니다.

① 본인확인기관으로 지정된 민간 기업들에게 주민등록번호가 과도하게 집적, 보관되어 외부에 유출될 위험성이 점증합니다.

이미 게시판실명제 위헌결정에서 헌법재판소는 “정보통신서비스 제공자에 대한 본인확인정보 보관의무 부과로 인하여 게시판 이용자의 개인정보가 외부로 유출되거나 부당하게 이용될 가능성”을 들어 그와 같은 보관의무를 전제로 한 게시판실명제에 대해 개인정보자기결정권의 침해라고 판단한 바 있습니다.

앞서 언급한 정보통신서비스 제공자의 대규모 주민등록번호 유출사고 사례에서도 알 수 있듯이 일단 정보통신서비스 제공자들이 주민등록번호를 대규모로 보관하고 있는 이상 개인정보 유출 사고에서 자유로울 수 없습니다. 헌법재판소가 게시판실명제 위헌 결정에서 게시판 실명제가 개인정보자기결정권을 침해하고 있다고 판단한 가장 큰 근거도 정보통신서비스의 특성 상 이용자가 대규모라는 점, 개인정보를 보관하는 정보통신서비스 제공자의 범위가 늘어날 수록 집적되는 개인정보는 천문학적인 규모라는 점을 고려한 것입니다.

정보통신망법은 민간영역에서 활용될 ‘대체수단’을 개발하기 위해 본인확인기관을 두고 있으므로 본인확인기관이 제 역할을 수행하기 위해서는 본인확인기관들이 거의 대부분의 국민들에게 대체수단을 제공할 수 있어야 합니다. 따라서 본인확인기관들은 정보통신망법 상 지정 목적을 달성하기 위해서는 필연적으로 가능한 많은 국민의 개인정보를 보관하고 있어야 하는 것입니다. 본인확인기관이 제 역할을 수행하면 할수록 집적되는 개인정보의 양은 이에 비례하여 늘어나서 결국

천문학적으로 증가할 것임은 별도의 사실관계를 확인하지 않고서도 충분히 예측 가능합니다. 따라서 본인확인기관이 목적 달성을 위해 거의 대부분의 국민의 주민등록번호 및 개인정보를 집적 보관하게 되면 게시판실명제 하에서 정보통신 서비스 제공자에 의하여 보관되던 개인정보에 비하여 보관되는 그 규모는 비교할 수도 없이 커지게 되며, 이 사건 범조항은 게시판 실명제 위헌결정과 같은 이유로 개인정보자기결정권을 본질적으로 침해하고 있는 것입니다.

실제로 대부분의 국민들이 일상생활에서 이동통신서비스를 사용하고 있으며, 본인확인기관으로 지정된 이동통신사 간 번호 이동이 일상화되어 있는 점에 비추어 보면 개별 이동통신사들은 거의 전 국민의 주민등록번호를 수집하고 있다고 볼 수 있습니다. 주식회사 케이티의 경우 이번 개인정보 유출사고를 통해 인하여 무려 1,200만 명의 개인정보를 유출시켰다는 점은 이를 방증하고 있다고 할 것입니다. 특히 이 사건 범조항으로 인하여 본인확인기관은 '주민등록번호'까지 합법적으로 수집할 수 있게 되어 유출사고가 일어날 경우 주민등록번호까지 함께 유출될 위험성을 배태하고 있었는데, 이번 주식회사 케이티에 대한 해킹 사건을 통하여 주민등록번호가 대량 유출 가능성이 현실화되었다고 할 것입니다.

본인확인기관인 주식회사 케이티의 개인정보 유출 사건 이외에도 정보통신망을 통한 주민등록번호 유출 사례는 계속 발생되고 있으며, 한번 침해된 주민등록번호는 이를 이용한 2차 피해로 이어져 끊임없이 개인정보자기결정권 침해가 재생산되고 있습니다.

최근 10여 년간 정보통신서비스 제공자에 의해 주민등록번호가 유출된 사례만 요약해도 다음과 같습니다.

○2001년 네띠앙 회원 15만명 등 27개 인터넷 업체들이 930만 건의 고객 개인정보(이름, 주민등록번호, 집·직장주소, 전화번호, 이메일 주소)를 두 개의 카드

사와 한 개의 생명보험사에 불법 판매한 사건

○2001년 BC카드, 국민카드, 다이너스 카드가 고객 개인정보(이름, 주민등록번호, 주소, 전화번호, 카드번호, 이용한도)를 보험사에 불법 판매한 사건

○2003년 SK가 자사가 보유한 1,700만명의 OK 캐쉬백 가입자들의 개인정보(이름, 주민등록번호, 집전화번호, 휴대전화번호, 주소)를 신한생명에 제공한 사건

○2005년 SK텔레콤 가입자 개인정보 95건, KTF 42건, LG텔레콤 35건, KT 28건 등 총 200여건의 개인정보를 심부름센터 등에 판매한 사건

○2005년 NC소프트의 리니지 계정과 비밀정보 유출 사건으로 경찰 측 추산 122만 건의 주민등록번호 도용 피해가 발생한 사건

○2006년 KT, 하나로, 두루넷, 온세통신 771만명의 가입정보(이름, 주민등록번호 등)를 시중에 불법 유출한 사건

○2008년 인터넷 경매사이트 옥션의 1,863만 명의 고객 개인정보(이름, 주민등록번호, 주소, 전화번호, 계좌번호 등)의 해킹 사건

○2008년 GS칼텍스 직원의 고객 인터넷 누리집 가입회원 1,151만 명의 개인정보(이름, 주민등록번호, 주소, 이메일 등) 유출 사건

○2010년 중국 해커로부터 구입된 25개 온라인 사이트(아이러브스쿨, 대명리조트, 러쉬앤 캐쉬, 현대캐피탈, 씨티파이낸셜, 제일캐피탈, 하나캐피탈 등)의 회원 개인정보(이름, 아이디, 비밀번호, 주민등록번호) 2,000만 건이 시중에 유통된 사건

○2011년 온라인 게임사인 넥슨의 메이플스토리의 백업서버 해킹으로 이용자 1,320만 명의 개인정보(이름, 주민등록번호, 아이디, 비밀번호)가 유출된 사건

○2011년 SK커뮤니케이션즈의 네이트, 싸이월드 회원 3,500만 명의 개인정보(이름, 주민등록번호, 아이디, 비밀번호 등)가 해킹되어 유출된 사건

○2011. 2.경부터 2012. 7.경까지 KT휴대전화 가입자 870만 명의 주민등록번호 등 고객정보가 유출된 사건

○2013년 SC, 씨티은행이 금융권 개인정보(이름, 전화번호, 주민등록번호, 직장명, 대출금액, 대출금리, 대출계좌, 카드번호 등)를 대출모집인에게 60만 건 유출한 사건

○2014년 KB 국민카드에서 5,300만 건, 롯데카드에서 2,600만 건, NH농협카드에서 2,500만 건 등 약 1억 400만 건의 개인정보(이름, 이메일, 휴대전화번호, 직장, 집 전화번호, 주민등록번호, 직장주소, 자택주소, 직장정보, 주거상황, 카드이용실적, 카드결제계좌, 카드결제일, 카드신용한도, 카드신용등급 등)가 유출된 사건

○2014년 네이버 가입자의 개인정보(아이디, 비밀번호, 주민등록번호) 20만 건 해킹 유출된 사건 등 그 피해사례를 일일이 열거하기 어려울 정도입니다.

② 이 사건 법조항은 본인확인기관의 주민등록번호 처리 원칙을 전혀 규율하고 있지 않으며, 개인정보처리 원칙이 충족되지 않는 경우에도 본인확인기관으로 하여금 주민등록번호 처리를 금지할 수 없습니다.

이 사건 법조항은 본인확인기관에 주민등록번호 사용이라는 기본권 침해 소지가 매우 큰 권한을 부여하고 있으면서도 본인확인기관이 주민등록번호 처리 과정에서 준수해야 할 개인정보처리 원칙의 세부 내용을 전혀 규율하고 있지 않습니다. 즉, 수집된 주민등록번호가 본인확인기관 내에서는 어떻게 사용되는지 그리고 본인확인기관과 계약을 맺은 다른 주체들과의 관계에서 어떻게 사용되는지에 대해 이용자는 전혀 알지 못하며, 이에 대해서 어떠한 통제 권한을 가지고 있지 못하므로 이 사건 법조항은 청구인의 개인정보자기결정권을 침해합니다.

또한 개인정보 유출 등의 사유로 해당 본인확인기관이 더 이상 주민등록번호 처리에 필요한 개인정보처리원칙을 준수하고 있지 않는 경우에 주민등록번호에 대한 정보처리금지청구권이나 정보삭제청구권 역시 전혀 구체화하고 있지 않고 있습니다

개인정보자기결정권을 구성하는 정보처리금지청구권과 정보삭제청구권은 기본적인 정보처리 원칙이 충족되지 않는 경우에는 개인정보의 이용·제공 등의 정보처리를 금지하거나 삭제하도록 요구할 수 있는 것을 주요 내용으로 하고 있습니다. 즉 개인정보가 유출되는 등 기본적인 정보처리 원칙이 충족되지 않는 경우에 청구인과 같은 이용자는 개인정보 처리의 금지 또는 삭제를 요구할 수 있는 권리를 가지고 있는 것입니다. 이미 살펴본 바와 같이 주민등록번호가 정보통신망을 통해 유출되는 경우에 담당 행정청 및 법원은 이를 주민등록번호의 정정사유로 인

정하고 있지 않기 때문에, 헌법이 보장하는 정보처리금지청구권을 이용하여 더 이상 해당 본인확인기관이 주민등록번호의 처리 금지나 삭제를 요청해야 할 필요성은 더욱 크다고 할 것입니다. 그럼에도 불구하고 주민등록번호가 유출된 경우 이 사건 법조항은 본인확인기관으로 하여금 주민등록번호를 더 이상 사용하지 못하도록 하는 것을 내용으로 하는 정보처리금지청구권이나 정보삭제청구권을 규율하고 있지 않아 청구인의 개인정보자기결정권을 침해하고 있습니다.

3) 소결

이미 살펴본 바와 같이 이 사건 법조항은 명확성 원칙이나 목적구속성 원칙도 충족하지 않고 있어 이 사건 법조항으로 인하여 달성되는 공익 자체가 특정되지 않고 있습니다. 즉, 이 사건 법조항으로 인하여 달성되는 공익은 거의 없거나 불명확한 반면 이로 인하여 침해되는 청구인의 개인정보자기결정권은 본질적이므로 법익균형성의 원칙도 충족하지 않습니다.

VI. 결론

주민등록번호는 모든 국민에게 강제적으로 부여되는 개인식별번호로서 한번 부여되면 매우 예외적인 상황이 아니면 변경할 수 없으며, 주민등록번호 제도 자체가 위헌성을 배태하고 있어 도입목적인 행정목적 외 민간활용은 엄격히 제한되어야 합니다.

요컨대 주민등록번호는 정보통신망서비스 회원으로 가입하는데 사용되어서는 안 될 성격의 고유식별번호입니다. 정보통신망법 제23조의2 제1항의 “정보통신서비스 제공자에 대한 주민등록번호 수집금지 원칙”은 이 같은 개인정보자기결정권의 내용을 구체적으로 기술한 것입니다. 그러나 주민등록번호를 아무런 제한 없

이 민간에서 활용할 수 있는 예외를 허용하고 있는 이 사건 법조항은 청구인의 개인정보자기결정권을 침해하여 헌법에 위반됨이 명백하다고 할 것입니다.

첨부서류

1. 청구인의 개인정보 유출 내역 확인 화면 캡처 (주식회사 케이티 제공)
2. kt 개인정보 유출확인, 주민등록번호 또 입력하라는 안내에 네티즌들 “폭발”, 조선일보 (2014. 3. 11.)
3. <개인정보자기결정권의 제한과 전자여권>, 이상명, 법학논총, 한양대학교 법학연구소 (2008)
4. <온라인상 주민등록번호 수집금지 정책의 시행과 쟁점>, 심우민, 국회입법조사처, 이슈와 논점 제614호 (2013. 3. 4.)
5. <개인정보 유출사고와 본인확인기관 활용의 문제점>, 심우민, 국회입법조사처, 이슈와 논점 제814호 (2014. 3. 17.)

2014. 6.

청구인의 대리인
변호사 박지환 (인)

헌법재판소 귀중