헌법소원심판청구서

청 구 인　　1. 김 승 현

청 구 인　　2. 추 미 선

위 청구인들의 대리인 변호사 김 가 연

서울 서초구 서초대로 50길 62-9, 402호 (사)오픈넷

전화 : 02) 525 - 2082,　팩스 : 02) 581 - 1642

청 구 취 지

"전기통신사업법(법률 제14839호로 개정된 것) 제32조의4 제2항, 제3항, 제4항과 제32조의5는 헌법에 위반된다."라는 결정을 구합니다.

침해된 권리

헌법 제18조 통신의 자유, 제17조 사생활의 비밀과 자유, 개인정보자기결정권

침해의 원인

전기통신사업법 제32조의4 제2항, 제3항, 제4항, 제32조의5

청 구 이 유

I. 청구인들의 지위

청구인들은 이동통신사와 전기통신역무 제공에 관한 계약을 체결하는 과정에서 전기통신사업자에게 부정가입방지시스템 등을 이용하여 본인 여부를 확인하도록 하고 있는 전기통신사업법 제32조의 4 제2항, 제3항, 제4항, 제32조의5(이하 “이 사건 본인확인 의무 조항”이라 합니다)에 의하여 익명 통신의 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 침해받고 있는 사람들입니다.

1. 청구인 1

청구인 1은 2017. 9. 20. SK Telecom 대리점에서 삼성 갤럭시 S8 휴대폰 사용을 위한 전기통신역무 제공에 관한 계약을 체결하고자 했습니다. 대리

점 직원이 본인 여부 확인이 필요하다는 이유로 청구인 1에게 신분증을 요구하여 청구인 1은 주민등록증을 제시했으며, 부정가입방지시스템을 통해 본인이라는 점이 확인이 된 후에야 계약을 체결할 수 있었습니다

2. 청구인 2

청구인 2는 2017. 10. 19. KT 대리점에서 익명으로 전기통신역무 제공에 관한 계약을 체결하고자 했습니다. 직원이 본인 여부 확인이 필요하다는 이유로 신분증을 요구하자 청구인 2는 신분증 제시 없이 익명으로 계약을 체결할 수 있는지 문의했으나 본인 확인이 되지 않을 경우 계약의 체결을 거부할 수 있다는 답변을 듣고 결국 계약을 체결하지 못하였습니다.

II. 헌법소원심판의 요건

1. 관련 규정 - 공권력의 행사

제32조의4(이동통신기기 부정이용 방지 등) ① 생략

② 전기통신역무의 종류, 사업규모, 이용자 보호 등을 고려하여 대통령령으로 정하는 전기통신사업자는 전기통신역무 제공에 관한 계약을 체결하는 경우(전기통신사업자를 대리하거나 위탁받아 전기통신역무의 제공을 계약하는 대리점과 위탁점을 통한 계약 체결을 포함한다) 계약 상대방의 동의를 받아 제32조의5제1항에 따른 부정가입방지시스템 등을 이용하여 본인 여부를 확인하여야 하고, 본인이 아니거나 본인 여부 확인을 거부하는 경우 계약의 체결을 거부할 수 있다. 전기통신역무 제공의 양도, 그 밖에 이용자의 지위승계 등으로 인하여 이용자 본인의 변경이 있는 경우 해당 변경에 따라 전기통신역무를 제공받으려는 자에 대하여도 또한 같다.

③ 제2항에 따라 본인 확인을 하는 경우 전기통신사업자는 계약 상대방에게 주민등록증, 운전면허증 등 본인임을 확인할 수 있는 증서 및 서류의 제시를 요구할 수 있다.

④ 제2항에 따른 본인 확인방법, 제3항에 따른 본인임을 확인할 수 있는 증서 및 서류의 종류 등에 필요한 사항은 대통령령으로 정한다.

제32조의5(부정 가입 방지 시스템 구축) ① 과학기술정보통신부장관은 부정한 방법을 통한 전기통신역무 제공계약 체결을 방지하기 위하여 가입자 본인 확인에 필요한 시스템(이하 "부정가입방지시스템"이라 한다)을 구축하여야 하고, 제32조의4제2항에 따른 전기통신사업자가 해당 시스템을 이용할 수 있도록 하여야 한다.

② 과학기술정보통신부장관은 부정가입방지시스템의 구축·운영을 위하여 본인(법정대리인을 포함한다) 확인에 필요한 다음 각 호의 정보를 보유한 국가기관·공공기관의 장에게 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 제32조의4제3항에 따라 제시한 증서 등의 진위 여부에 대한 확인을 요청할 수 있다. 이 경우 요청을 받은 국가기관·공공기관의 장은 정당한 사유가 없으면 이에 따라야 한다.

1. 개인의 주민등록 및 가족관계에 관한 정보
2. 법인의 등기 및 사업자등록에 관한 정보
3. 외국인과 재외국민의 등록·거소신고 및 출입국에 관한 정보
4. 그 밖에 제32조의4제3항에 따라 제시한 증서 및 서류에 관한 정보

③ 과학기술정보통신부장관은 부정가입방지시스템의 구축·운영 등의 업무를 대통령령으로 정하는 바에 따라 「방송통신발전 기본법」 제15조에 따른 한국정보통신진흥협회(이하 "한국정보통신진흥협회"라 한다)에 위탁할 수 있다.

2. 이 사건 심판청구의 적법요건

가. 기본권 침해의 자기관련성·현재성

청구인들은 이 사건 본인확인 의무 조항으로 인하여 익명으로 이동통신서비스를 사용할 수 없게 되어 기본권을 침해받고 있으므로 자기관련성과 현재성이 인정됩니다.

이 사건 본인확인 의무 조항은 본인확인 의무를 전기통신사업자에게 부과하고 있는 것처럼 보이지만, 본임임을 확인할 수 있는 증서 및 서류의 제시를 할 실질적인 의무는 계약 상대방인 이용자에게 직접 부과됩니다. 따라서 청구인들은 공권력 행사의 직접적인 상대방이라 할 것입니다.

설령 청구인들이 직접적인 상대방이 아닌 제3자라고 하더라도 공권력 작용이 그 제3자의 기본권을 직접적이고 법적으로 침해하고 있는 경우에는 예외적으로 자기관련성이 인정될 수 있습니다. 이런 취지에서 인터넷 게시판을 설치·운영하는 정보통신서비스 제공자에게 게시판 이용자로 하여금 본인확인절차를 거쳐야만 게시판에 정보를 게시할 수 있도록 하는 조치를 마련할 의무를 부과하는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'의 경우 게시판 이용자에게 자기관련성이 인정되었습니다(헌재 2012. 8. 23. 2010헌마47, 252(병합) 참조). 이와 마찬가지로 청구인들의 자기관련성이 인정된다 할 것입니다.

또한 법령에 대한 헌법소원의 청구기간은 법령이 시행된 뒤에 비로소 기본권을 침해받은 경우에는 기본권을 침해받은 때로부터 기산해야 하는데, 이 사건의 경우 청구인들이 이동통신사와 전기통신역무 제공에 관한 계약을 체결하고자 하면서 본인확인을 요구받았을 때 기본권의 침해가 발생했다 하겠습니다. 청구인 1은 2017. 9. 20. 계약을 체결하고 실명으로 휴대폰을 사용하고 있으므로 현재성이 인정되며, 청구인 2는 2017. 10. 19. 익명으로 계약을 체결하고자 하였으나 거부당하여 익명으로 휴대폰을 사용하지 못하고 있으므로 현재성이 인정됩니다.

나. 직접성

이 사건 본인확인 의무 조항은 전기통신사업자를 대상으로 계약 상대방의 본인 여부를 확인할 의무를 부과하여 청구인들의 기본권을 직접적으로 침해하고 있습니다.

법률 또는 법률조항 자체가 헌법소원의 대상이 되기 위해서는 그 법률 또는 법률조항에 의하여 구체적인 집행행위를 기다리지 않고 법률 자체에 의하여 자유의 제한, 의무의 부과, 권리 또는 법적 지위의 박탈이 생긴 경우여야 합니다. 그러나 구체적 집행행위가 존재하는 경우라고 하여 언제나 반드시 법률자체에 대한 헌법소원심판청구의 적법성이 부정되는 것은 아니며, 예외적으로 집행행위가 존재하는 경우라도 그 집행행위를 대상으로 하는 구제절차가 없거나 구제절차가 있다고 하더라도 권리구제의 기대가능성이 없고, 다만 기본권침해를 당한 청구인에게 불필요한 우회절차를 강요하는 것밖에 되지 않는 경우 등으로서 당해 법률에 대한 전제관련성이 확실하다고 인정되는 때에는 당해 법률을 헌법소원의 직접 대상으로 삼을 수 있습니다(헌재 1992. 4. 14. 90헌마82; 헌재 1997. 8. 21. 96헌마48 등).

이 사건 본인확인 의무 조항은 전기통신사업자를 대상으로 계약 상대방의 본인 여부를 확인할 의무를 부과하고 있습니다. 이러한 의무는 중간에 어떠한 집행행위의 개입이 없이 법조항 그 자체에 근거한 것이며, 이에 의해 청구인들은 직접적으로 기본권을 침해받고 있습니다.

다. 보충성

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

라. 권리보호이익

청구인들은 이 사건 본인확인 의무 조항으로 인하여 기본권을 침해받고 있으며, 위 조항이 위헌으로 결정될 경우 청구인은 위와 같은 기본권의 제한에서 벗어날 수가 있으므로 이 사건 심판청구는 권리보호이익이 있다 할 것입니다.

마. 청구기간

헌법재판소법 제69조 제 1항은 “제68조 제1항의 규정에 의한 헌법소원의 심판은 그 사유가 있음을 안 날부터 90일 이내에, 그 사유가 있은 날부터 1년 이내에 청구하여야 한다.”하여 청구기간에 대하여 규정하고 있습니다. 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 것입니다(헌재 2002. 1. 31. 2000헌마274 참조).

청구인 1은 2017. 9. 20. 전기통신서비스 제공 계약을 체결하여 이때 비로소 법령에 해당하는 사유가 발생하였고, 청구인 2는 2017. 10. 19. 이 사건 본인확인 의무 조항으로 인하여 자신의 기본권이 제한받고 있다는 것을 알게 되었습니다.

결론적으로 청구인들은 모두 자신의 기본권이 침해되고 있다는 사실을 안 날로부터 90일, 그 사유가 있은 날부터 1년이 경과하지 않았으므로 이 사건 심판청구는 청구기간을 준수하였습니다.

바. 소 결

이 사건 심판청구는 자기관련성, 현재성 등의 요건을 충족하고 있으며, 그 밖에 직접성, 보충성, 권리보호의 이익, 청구기간 등의 요건을 모두 갖추고 있으므로 적법합니다.

III. 이 사건 심판대상의 위헌성

1. 이 사건 본인확인 의무 조항에 의하여 제한되는 기본권

이 사건 본인확인 의무 조항은 전기통신사업자가 전기통신역무 제공에 관한 계약을 체결하는 과정에서 부정가입방지시스템 등을 이용하여 계약 상대방의 본인 여부를 확인하는 '본인확인제' 즉 '휴대폰 실명제'를 규정하고 있어 익명 통신의 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 제한합니다.

가. 익명 통신의 자유의 제한

(1) 익명 통신의 자유의 의의

헌법 제18조는 "모든 국민은 통신의 비밀을 침해받지 아니한다"라고 하여, 통신의 비밀보호를 그 핵심내용으로 하는 통신의 자유를 기본권으로 보장하고 있습니다. 통신의 자유를 기본권으로서 보장하는 것은 사적 영역에 속하는 개인간의 의사소통을 사생활의 일부로서 보장하겠다는 취지에서 비롯된 것입니다. 통신은 기본적으로 개인과 개인 간의 관계를 전제로 하지만, 통신의 수단인 우편이나 전기통신의 운영이 전통적으로 국가독점에서 출발하였기 때문에, 통신의 영역은 다른 사생활의 영역에 비하여 국가에 의한 침해 가능성이 매우 큰 영역입니다. 이에 따라 국가,

특히 수사기관에 의한 통신의 비밀에 대한 침해를 규제하기 위하여 '통신비밀보호법'이 제정되었습니다(헌재 2001. 3. 21. 2000헌바25).

헌법 제18조에서 그 비밀을 보호하는 '통신'의 일반적인 속성으로는 '당사자간의 동의', '비공개성', '당사자의 특정성' 등을 들 수 있는바, 이를 염두에 둘 때 위 헌법조항이 규정하고 있는 '통신'의 의미는 '비공개를 전제로 하는 쌍방향적인 의사소통'이라고 할 수 있습니다(헌재 2001. 3. 21. 2000헌바25). 그리고 통신의 비밀보호의 대상은 통신의 내용뿐만 아니라 통신의 당사자(수신인과 발신인), 수신지와 발신지, 정보의 형태, 발신횟수 등 통신과 관련된 일체를 포괄합니다. 따라서 수사기관이 통신의 내용, 전기통신사실에 관한 자료, 통신 당사자의 개인정보 등을 제공받기 위해서는, 즉 통신의 자유를 제한하는 경우에는 헌법상 영장주의의 원칙이 적용되어 법원의 영장 내지 허가를 필요로 합니다.

이러한 특성상 통신의 자유는 상대방 및 제3자에게 신원을 밝히지 않고 익명으로 통신할 자유인 '익명 통신의 자유'를 당연히 포함한다고 하겠습니다.

(2) 익명 통신의 자유와 익명 표현의 자유

통신의 자유는 표현의 자유와 마찬가지로 외면적 정신활동의 자유이며, 다만 그 표현이 의해 구별될 수 있습니다. 통신의 비밀보호는 개인의 사상과 정보의 자유로운 전달을 보호함으로써 정보통신의 발전에 따라 오늘날 수많은 표현행위와 정보 교환이 이메일, 카카오톡, 트위터 등 정보통신 수단에 의해 이루어짐을 고려할 때, 디지털 사회에서 통신의 자유는 표현의 자유 보장의 전제조건으로 기능하고 있습니다. 이렇게 통신의 자유와 밀접한 관계에 있는 표현의 자유에 대해 헌법재판소는 "자신의 신원을 누구에게도 밝히지 아니한 채 익명 또는 가명으로 자신의 사상이나 견해를 표명하고 전파할 익명표현의 자유도 그 보호영역에 포함된다"는 점을 분명히 하였습니다(헌재 2012. 8. 23. 2010헌마47, 252(병합), 헌재

2010. 2. 25. 2008헌마324 등).

‘익명 표현의 자유’와 ‘익명 통신의 자유’는 국제인권법상으로도 인정받는 인권입니다. 대한민국이 1990. 4. 10. 비준한 ‘시민적·정치적 권리에 관한 국제규약’(The International Covenant on Civil and Political Rights, 이하 “규약"이라고 합니다)에서는, 의사의 자유(규약 제19조 제1항)와 표현의 자유(규약 제19조 제2항)를 보장해야 할 당사국의 의무를 규정하고 있습니다. 유엔의 핵심 인권 기구인 유엔 인권이사회에서는 의사표현의 자유가 “인권과 자유의 향유에 있어 본질적인 것이며, 민주주의 사회의 건설 및 강화를 위한 근간을 이룬다”라고 천명하였습니다.

위 규약은 익명성에 대하여 명시적으로 언급하고 있지는 않지만, 그 입안과정을 보면, 입안자들이 익명성을 표현의 자유에 있어서 중요한 것으로 보았음을 알 수 있습니다. 이러한 논의과정 중에서 당사국들은 규약 제19조 제1항에 “익명성은 허용되지 않는다”라는 문구를 추가하는 방안에 반대하였는데, 이는 “저자를 보호하기 위해 익명성이 필요할 수 있다”, “그러한 익명성 불허 문구는 필명 사용을 제한할 수 있다”라는 점을 고려한 것입니다.[1)]

현 유엔 의사표현의 자유 특별보고관 데이비드 케이(David Kaye)는 2016헌마388 사건에 관해 헌법재판소에 제출한 제3자 의견서에서 다음과 같이 말했습니다. “익명 통신은 그것 자체로서 규약 제19조 제2항에 의하여 보호되는 표현 활동이 될 수 있습니다. 현대 문화에서 가이포크스(Guy Fawkes) 마스크 착용은 시위에 참여하는 자의 정체를 숨기고 정치적인 진술을 하게 하는 두 가지 기능을 모두 수행합니다. 즉, 자신의 정체를 숨기는 행위 자체가 의사표현의 한 형태일 수 있습니다.”(첨부서류 1. 유엔 의사표현의 자유 특별보고관 헌재 의견서 참조)

또한 특별보고관은 2015년 5월 22일 발표한 ‘디지털 통신에서의 암호화와 익명성’에 관한 보고서에서, 암호화와 익명성은 의견과 신념을 보호하

1) Marc J. Bossuyt, *Guide to the “Travaux Préparatoires” of the International Covenanton Civil and Political Rights,* Feb. 17, 1987, 379-80면.

는 프라이버시 영역을 형성해 사적 통신을 가능케 하고 의견을 외부의 평가로부터 보호할 수 있게 하며, 이는 특히 적대적인 정치적·사회적·종교적·법적 환경에서 더욱 중요하다고 하면서, 각 국가는 암호화와 익명성을 옹호해야 하며 원칙적으로 제한하지 말 것을 권고한 바 있습니다. 이러한 권고는 이전 유엔 의사표현의 자유 특별보고관 프랭크 라 뤼가 2013년 4월 발표한 국가 감시에 관한 보고서의 권고 사항과도 일치합니다.

(3) 이 사건의 경우

이 사건 본인확인 의무 조항은 누구든지 전기통신역무를 이용하고자 하는 사람은 본인여부를 확인받게 하고, 확인이 되지 않는 경우 전기통신사업자가 전기통신역무의 제공을 거부하게 함으로서 이용자가 익명으로 통신할 가능성을 원천적으로 차단하고 있어 익명 통신의 자유를 제한합니다.

나. 사생활의 비밀과 자유의 제한

(1) 사생활의 비밀과 자유의 의의

'사생활의 자유'란, 사회공동체의 일반적인 생활규범의 범위 내에서 사생활을 자유롭게 형성해 나가고 그 설계 및 내용에 대해서 외부로부터의 간섭을 받지 아니할 권리로서, 사생활과 관련된 사사로운 자신만의 영역이 본인의 의사에 반해서 타인에게 알려지지 않도록 할 수 있는 권리인 '사생활의 비밀'과 함께 헌법상 보장되고 있습니다(헌재 2001. 8. 30. 99헌바92 등).

프라이버시권이라고도 하는 사생활의 비밀과 자유는 사생활의 평온을 침해받지 아니하고 사생활의 비밀을 함부로 공개당하지 아니할 소극적 권리와 자신에 관한 정보를 관리·통제할 수 있는 적극적 권리를 포함합니다. 프라이버시권의 적극적인 측면은 개인정보자기결정권으로 발현된다 할 것입니다.

이에 따라 이용자가 전기통신역무를 이용하여 자유롭게 사적으로 의사소통할 권리는 당연히 사생활의 자유에 의해 보호되며, 사적으로 의사소통한 내용 그리고 했다는 사실 자체도 타인에게 알려지지 않도록 할 수 있는 권리는 사생활의 비밀에 의해 보장된다 할 것입니다. 특히 인터넷 본인확인제 위헌 결정(헌재 2012. 8. 23. 2010헌마47, 252(병합))의 취지에 따르면, 통신은 상호 동의하에 이루어지는 사적인 의사표현으로 공개적인 의사표현에 비해 더욱 두텁게 보호되어야 합니다. 명예훼손적 표현 등 불법정보의 급속한 확산과 같은 피해가 존재하지 않기 때문입니다.

(2) 감시기술의 발전과 프라이버시 침해

정보통신 기술의 발전은 과거에는 상상할 수 없을 만큼 통신수단, 거리, 시간에 구애받지 않는 자유로운 의사소통과 정보공유를 가능케 해 표현의 자유, 통신의 자유, 알 권리 등 정보인권을 신장시켜왔습니다. 하지만 이와 함께 감시·추적 기술도 발전하여 비단 국가에 의해서 뿐만 아니라 기업과 사인에 의해서도 개인의 프라이버시가 부당하게 침해되는 사례가 급증하고 있습니다.

특히 온라인에서 이루어지는 모든 통신과 표현행위는 기록을 남기기 때문에 용이하게 감시가 가능하므로, 우리나라와 같이 스마트폰 보급률과 인터넷 가입률이 높은 나라에서는 전 국민이 감시와 추적의 대상이라고 해도 과언이 아닙니다. 이는 프라이버시에 대한 중대한 제한이며, 휴대폰 실명제는 모든 휴대폰을 이용자의 실제 신원과 연계시킴으로써 이러한 제한을 더욱 가중시키는 것입니다.

예컨대 휴대폰이 생성하는 정보는 비단 통화나 문자에 관한 정보뿐만 아니라, 위치정보, GPS 정보, IP 주소 등 인터넷 접속 정보와 같은 다양한 정보를 포함하며, 이통사는 각 디바이스의 이용자의 신원정보를 갖고 있기 때문에, 마음만 먹으면 휴대폰 사용으로 수집된 정보와 신원정보의 결합을 통해 이용자가 어디를 다녀 왔는지, 누구랑 연락을 주고 받았는

지, 인터넷에 언제 얼마나 접속했는지 등 사생활에 관한 내용을 간단히 알아낼 수 있습니다.

(3) 이 사건의 경우

이 사건 본인확인 의무 조항은 누구든지 전기통신역무를 이용하고자 하는 사람은 본인 여부를 확인받도록 강제함으로써 이용자의 사생활의 비밀과 자유를 제한하고 있습니다.

다. 개인정보 자기결정권에 대한 제한

개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리입니다.

개인정보자기결정권의 보호대상이 되는 개인정보는 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 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당합니다(헌재 2005. 5. 26. 99헌마513, 2004헌마190(병합)).

이 사건 본인확인 의무 조항은 전기통신사업자가 전기통신역무를 이용하고자 하는 정보주체의 이름, 주민등록번호, 주소 등 본인확인정보를 조사하고 수집·보관하게 할 의무를 지우고 있는데, 본인확인정보는 개인의 동일성을 식별할 수 있게 하는 정보로서 개인정보자기결정권의 보호대상이 되는 개인정보에 해당하므로, 결국 이 사건 본인확인 의무 조항은 이용자의 개인정보자기결정권을 제한하고 있습니다.

2. 이 사건 본인확인 의무 조항의 기본권 침해

이 사건 본인확인 의무 조항은 청구인들의 익명 통신의 자유, 사생활의 비밀과 자유 그리고 개인정보자기결정권을 제한하는 바, 헌법 제37조 제2항에 규정된 기본권 제한의 한계를 준수할 것이 요구됩니다. 그러나 아래에서 보는 바와 같이 이 사건 본인확인 의무 조항은 과잉금지의 원칙에 위반하여 청구인들의 기본권을 침해하고 있습니다.

가. 입법목적의 정당성

오늘날 눈부신 정보통신기술의 발전과 높은 휴대폰 보급률과 함께 타인명의 휴대폰, 소위 '대포폰' 이용한 사기 등 범죄가 증가하고 있어, 이러한 휴대폰의 부정이용을 방지하기 위해 전기통신사업자에게 본인확인 의무를 부과하여 범죄를 예방하고 수사를 용이하게 하자는 이 사건 본인확인 의무 조항의 입법 목적의 정당성은 인정할 수 있다고 하겠습니다.

나. 수단의 적합성

하지만 휴대폰 부정이용의 방지라는 목적을 달성하기 위해 휴대폰을 이용하고자 하는 모든 사람의 본인 여부를 확인하는 것은 효과적이고 적절한 방법이라 하기 어렵습니다. 특히 이 사건 본인확인 의무 조항이 규정하는 전면적 본인확인제 또는 휴대폰 실명제는 기본권에 대한 제한이 너무 크기 때문에 적합한 수단이라 할 수 없습니다.

첫째, 휴대폰 실명제가 범죄 예방에 효과적이라는 증거는 찾아볼 수 없습니다. 계획적으로 범죄를 도모하는 자는 어차피 타인의 휴대폰을 빌려서 쓰거나, 차명으로 휴대폰을 개통하는 등의 방법으로 법망을 피해가고 있기 때문입니다. 이런 상황에서 모든 사람이 휴대폰을 본인 명의로 사용한다는 전제 하에 먼저 명의자를 용의자로 가정하고 수사하는 방식은 오

히려 수사를 지연시키기만 할 뿐입니다.

이러한 이유로 멕시코에서는 SIM카드 구매 시 의무적으로 본인정보를 등록하도록 하는 정책, 즉 SIM카드 등록제를 도입했다가 3년 만에 폐지했으며, 영국, 캐나다, 뉴질랜드, 체코공화국, 루마니아 등의 국가는 유사한 제도의 도입을 고려했다가 취소하기도 했습니다.[2] 그리고 2012년 EU 집행위원회(EC)의 세실리아 말스트롬(Cecilia Malström) 집행위원은 SIM 카드 등록제가 범죄수사 등에 특별한 편익을 가져다주지 않는다는 의견을 낸 바 있습니다.[3]

둘째, 사업자가 개인정보를 수집·보관하게 강제하는 각종의 본인확인제로 인해 그 동안 이동통신사, 인터넷 사업자, 금융업자 등 다양한 영역의 개인정보처리자들이 국민 대다수의 개인정보를 축적해왔는 바, 이로 인해 매년 대규모의 개인정보 유출사태가 계속 발생하고 있으며, 지난 5년간 방송통신위원회에 접수된 개인정보 유출 누적 인원수만 해도 약 7200만 명으로 집계되었습니다(첨부자료 2. 2017. 9. 27.자 뉴스1 기사). 이렇게 본인확인제는 개인정보 집적을 강제하여, 해킹 등을 통한 개인정보유출과 명의도용 등의 범죄의 위험을 높이는 역효과 즉 범죄예방이라는 목표를 반감시키는 효과를 내기 때문에 전혀 적합한 수단이라 할 수 없습니다.

셋째 전기통신사업법 제32조의4 제3항은 본인 확인을 하는 경우 본인임을 확인할 수 있는 증서 및 서류의 제시를 요구하고 있으며, 법 시행령에 의하면 본인확인 증서는 주민등록증, 운전면허증, 장애인등록증, 여권 등으로 한정적입니다. 여하한 사유로 신분증이 없는 국민의 경우에는 원칙적으로 휴대폰 사용이 불가능하게 하는 수단인 것입니다.

결국 휴대폰 실명제는 휴대폰 부정이용의 방지 및 범죄의 예방이라는 목적에 적합한 수단이라 할 수 없습니다.

---

2) GSMA, *The Mandatory Registration of Prepaid SIM Card Users*, November 2013, 10면.
3) GSMA, *The Mandatory Registration of Prepaid SIM Card Users*, November 2013, 10면.

다. 침해의 최소성

이 사건 본인확인 의무 조항과 같은 기본권 제한적 조치가 정당한 수단이 되기 위해서는, 설령 그것이 입법목적을 달성하기 위해 적절한 수단이라 하더라도 그 외에 보다 완화된 다른 수단이나 대안이 없는지 살펴보아야 할 것입니다. 그런데 이 사건 본인확인 의무 조항이 표방하는 휴대폰 부정이용 방지 및 범죄 예방이라는 입법목적은 휴대폰 실명제처럼 이용자의 익명통신의 자유나 개인정보자기결정권 등 기본권을 중대하게 제한하지 않는 다른 수단에 의해서도 충분히 달성할 수 있습니다.

첫째, 범죄자가 타인 명의의 휴대폰을 사용하여 범죄를 저지른 경우 범죄자를 바로 특정하기 어려울 수 있으나, 이러한 범죄자의 신원 은폐시도에 따른 특정의 어려움은 통상의 불법행위에서도 발생하는 문제로서 통화내역 확인, 기지국 수사, 위치추적 등 명의와 상관없이 휴대폰의 실사용자를 검거하는 수사기법이 충분히 잘 발달되어 있어 얼마든지 극복될 수 있습니다. 이렇게 덜 침해적인 수단이 있음에도 불구하고 예외 없는 실명제를 시행하는 것은 침해 최소성의 원칙에 어긋납니다.

둘째, 타인 명의 휴대폰 사용을 처벌하는 규정들이 이미 있습니다. 특히 전기통신사업법 제30조는 그 입법 취지와는 다르게 그 동안 대포폰 내지 차명폰 제공을 처벌하는 근거로 활용되어 왔습니다(2013. 9. 13. 선고 2013도6062 판결). 그리고 이 사건 본인확인 의무 조항과 함께 도입된 전기통신사업법 제32조의4 제1항은 제30조에 더해 자금의 제공 또는 융통을 조건으로 휴대폰을 개통하는 등의 행위를 금지하고 처벌하고 있습니다.

셋째, 헌법재판소는 타인에게 휴대폰을 이용하게 해줄 권리를 이미 확인한 바 있습니다. 전기통신사업법 제30조와 거의 동일한 내용인 구 전기통신사업법 제74조는 죄형법정주의에서 도출된 명확성의 원칙에 위배될 뿐만 아니라 위임입법의 한계를 일탈하였다는 이유로 위헌 결정을 받은 바 있습니다(헌재 2002. 5. 30. 2001헌바5). 이후 개정이 되긴 했지만, 대

통령령으로 규정하던 내용을 법률에 규정하고 있을 뿐, 위헌 결정의 이유가 되었던 명확성 원칙 위반 부분이 여전히 존재합니다. 여기서 중요한 점은 헌법재판소가 동 조항이 왜 명확성 원칙에 위반된다고 보았는가입니다.

헌법재판소는 “전기통신사업자가 제공하는 전기통신역무를 이용하여 타인의 통신을 매개하는 더 한층 발전된 전기통신역무의 제공이나 그 산업발전의 기초가 되는 새로운 기술과 장비의 연구·개발행위 등도 금지될 수 있고, 또한 대가의 수령 여부를 불문하고, 전화나 피씨(PC)통신 등을 위하여 개인이 그 전화기나 컴퓨터를 친지 또는 이웃에게 빌려주든지, 전자제품 매장에서 전시·판매용 전화기나 컴퓨터를 시용(試用)하도록 하는 것 등도 모두 금지행위에 해당하게 되는 것은 아닌가 하는 의문이 제기될 여지” 때문에 명확성의 원칙에 위배된다고 하였습니다(헌재 2002. 5. 30. 2001헌바5). 즉, 연구목적, 친지 이웃에게 빌려줄 목적 등으로 타인에게 휴대폰을 이용하게 할 자유가 있는데 그런 행위를 금지하는 것처럼 법률이 해석될 수가 있으니 명확성의 원칙에 위배된다고 한 것입니다. 그런데 이 사건 본인확인 의무 조항은 본인확인 필요 없이 합법적으로 타인의 휴대폰을 이용할 수 있는 경우가 충분히 있음에도 불구하고 전혀 예외를 전혀 두고 있지 않기 때문에 침해의 최소성에 위배됩니다.

이렇듯 현행법에 의하더라도 휴대폰 부정이용에 대한 제재수단이 이미 마련되어 있고, 현재의 기술수준에서 사후적으로 대포폰 사용자의 신원을 파악하기가 그리 어렵지도 않습니다. 본인확인 이외의 여러 규제 조항들의 엄정한 집행을 통하여 대포폰 단속 및 처벌이 실질적으로 이루어진다면 휴대폰 실명제 실시 이상의 높은 일반예방 효과를 기대할 수도 있을 것입니다.

결국 이 사건 본인확인 의무 조항은 그 입법목적인 범죄 예방 효과는 거의 없으면서 전 국민을 잠재적 범죄자로 취급하고 있는 것으로 기본권에 대한 침해가 가장 심대한 수단이라 할 것입니다. 헌법재판소가 인터넷

실명제를 위헌으로 판단한 이유 중 하나도 소수의 악플러를 잡기 위해 모든 국민에게 일괄적으로 실명 확인 의무를 부과하는 것은 "수사편의 등에 치우쳐 모든 국민을 잠재적 범죄자와 같이 취급"하는 것이었기 때문입니다(헌재 2012. 8. 23. 2010헌마47, 252(병합)).

결론적으로 휴대폰 실명제는 그 입법목적을 달성할 다른 덜 침해적인 수단이 있음에도 불구하고 목적달성에 필요한 범위를 넘는 과도한 제한을 하는 것으로서 침해의 최소성이 인정되지 않음이 명백합니다.

라. 법익의 균형성

(1) 비례성 원칙의 위반

이 사건 본인확인제 또는 휴대폰 실명제는 적합한 수단이 아니며 침해의 최소성이 인정되지 않을 뿐만 아니라, 그것이 달성하고자 하는 휴대폰 부정이용 방지 및 범죄 예방이라는 공익과 청구인들의 익명 통신의 자유, 사생활의 비밀과 자유, 그리고 개인정보자기결정권에 대한 제한 정도를 비교형량하여 보았을 때 그 정도가 과도하여 비례성의 원칙에도 위배됩니다.

헌법재판소는 인터넷 본인확인제에 대해서 표현의 자유에 대한 사전검열은 아니나 '사전제한'이라고 하였습니다(헌재 2012. 8. 23. 2010헌마47, 252(병합)). 본인확인정보를 입력하지 않으면 표현을 할 수 없었기 때문입니다. 헌법재판소는 '사전제한'의 경우에는 그 제도를 정당화하는 공익이 명백해야 한다고 하였습니다. 즉 법률이 달성하는 공익과 법률이 제한하는 사익을 비교형량할 때 더욱 공익에 엄중한 요구를 해야 한다고 한 것입니다. 이 사건 조항 역시 본인확인정보가 연계되어 있지 않으면 통신을 하지 못하도록 하는, 통신의 자유에 대한 '사전제한'에 해당하므로 역시 이 사건 조항이 달성하는 공익이 명백한지 살펴봐야 합니다. 이와 같은 심사기준을 염두에 두고 이익형량을 해야 할 것입니다.

유엔 의사표현의 자유 특별보고관도 '암호화와 익명성' 보고서에서 익

명성에 대한 전면적 금지(Blanket prohibitions)는 그 자체로서 비례성의 원칙을 충족하지 못한다고 하면서, 각 국가는 SIM 카드 등록제 등 이용자를 식별하는 제도의 도입을 삼가야 한다고 권고한 바 있습니다. 이와 같은 강제적인 SIM 카드 등록제는 합법적인 정부의 이해를 넘어 개인과 언론인을 감시할 수 있는 역량을 정부에 제공하여 국민의 기본권을 심각하게 제약하기 때문입니다.

(2) 전 국민을 잠재적 범죄자로 취급

먼저 휴대폰 실명제가 부정이용 방지나 범죄 예방에 얼마나 효과가 있는지는 밝혀진 바 없으므로, 결국 휴대폰 실명제를 통해 얻어지는 명백한 공익은 수사의 용이성입니다. 즉, 추후 휴대폰 이용자가 범죄를 저질렀을 경우 신속하게 신원을 파악할 수 있다는 것입니다. 하지만 이 정도의 공익만으로는 청구인들의 익명 통신의 자유와 사생활의 비밀과 자유에 대한 침해를 정당화할 수 없습니다.

수사의 용이성은 매우 극소수인 범죄자에게만 해당되는데, 이 사건 본인확인 의무 조항은 위에서 보았듯이 거의 전 국민에게 예외없이 적용되는 제도로 온 국민을 잠재적 범죄자로 취급하고 감시하는 것이나 마찬가지입니다. 외국의 경우 본인확인이나 SIM 카드 등록을 요구하지 않고 선불폰 사용을 허용하는 나라들이 많습니다.[4] 이는 차명폰 또는 익명폰이 범죄에 이용될 여지가 있긴 하지만, 그렇다고 하여 전 국민에 대한 감시를 구성하고 프라이버시를 중대하게 침해하는 휴대폰 실명제를 도입하는 것은 큰 부담이기 때문입니다. 그리고 도입한다고 해도 국가안보 등 중대한 공익이 전제됩니다. 폴란드는 2016년 테러방지법을 제정하면서 선불폰

4) CENTRE FOR POLICY RESEARCH ON SCIENCE AND TECHNOLOGY SIMON FRASER UNIVERSITY VANCOUVER가 2006년 발간한 *Privacy Rights and Prepaid Communication Services*에 따르면, OECD 24개국을 대상으로 조사한 결과, 개인정보를 제공함이 없이 선불 휴대폰을 개통할 수 있는 국가는 15개국(오스트리아, 벨기에. 캐나다, 체코, 덴마크, 그리스, 아일랜드, 멕시코, 네덜란드, 뉴질랜드, 폴란드, 포르투갈, 스페인, 스웨덴, 영국, 미국)으로 개인정보를 제공하고 선불 휴대폰을 개통하여야 하는 9개국(호주, 프랑스, 독일, 헝가리, 일본, 노르웨이, 슬로바키아, 남아공, 스위스)의 두 배 가까이 됩니다. 나아가 이 중 범죄 수사 등의 목적으로 전체 휴대폰 이용자의 전화번호 데이터베이스(IPND)를 이용하는 국가는 2개국(호주, 스위스)에 불과합니다.

SIM 카드 등록제를 도입해 2017년 2월부터 시행하고 있습니다. SIM 카드를 등록할 때 실명을 제시할 필요가 없고 SIM카드 양도가 자유로워 우리나라의 휴대폰 실명제보다 훨씬 완화된 방식임에도 불구하고 도입 당시부터 국가적 감시이며 익명 통신의 자유를 침해한다는 이유로 거센 반대에 부딪혔습니다.[5)]

이렇듯 범죄 수사에 있어 신원 확보가 쉬워진다는 이유로 전 국민을 대상으로 휴대폰 실명제를 실시하는 것은 지극히 행정편의적 사고에 해당하며 국민의 익명 통신의 자유와 프라이버시에 대한 중대한 침해로서 이 사건 본인확인 의무 조항은 법익의 균형성을 충족하지 못하고 있습니다.

(3) 사인에 의한 주민등록번호의 광범위한 수집 및 개인정보의 집적

이 사건 본인확인 조항은 전기통신사업자가 주민등록증, 운전면허증 등의 증서 및 서류로 본인 확인을 하도록 되어 있습니다. 이 과정에서 이통사는 필수적으로 가입자의 주민등록번호를 수집하고 있습니다. 광범위한 주민등록번호 수집으로 침해되는 청구인들의 개인정보자기결정권에 관한 사익이 수사의 용이성이란 구체적 공익에 비하여 결코 적지 않기 때문에 휴대폰 실명제는 비례성의 원칙에 위반됩니다.

특히 우리나라에서 주민등록번호는 “단순한 개인식별번호에서 더 나아가 표준식별번호로 기능함으로써, 개인에 관한 정보가 주민등록번호를 사용하여 구축되고 그 번호를 통해 또 다른 개인정보와 연결되어 결과적으로 개인정보를 통합하는 연결자(key data)”로 사용되고 있습니다. 더욱이 오늘날 현대사회는 인터넷의 발달과 전산화의 실시로 인해 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있게 되었기에, 이러한 사회적 상황에서 개인정보를 통합하는 연결자 기능을 하는 주민

5) Anna Obem, *9 controversies about obligatory prepaid registration*, 2017. 1. 31., <https://en.panoptykon.org/prepaid>

등록번호가 불법 유출 또는 오·남용되는 경우 개인의 사생활뿐만 아니라 생명·신체·재산까지 침해될 소지가 큽니다(헌재 2015. 12. 23. 2013헌바68, 2014헌마449(병합)).

실제로 이렇게 큰 가치를 지니게 된 주민등록번호는 지속적으로 범죄의 표적이 되고 있으며, 대규모의 정보 유출 사고가 지속적으로 발생하고 있습니다. 이렇게 유출된 주민등록번호는 다른 개인정보와 연계되어 각종 광고 마케팅에 이용되고 보이스피싱 등의 범죄에 악용되고 있으며, 심지어 그 자체가 거래의 대상이 되고 있습니다.

따라서 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 있습니다(헌재 2015. 12. 23. 2013헌바68, 2014헌마449(병합)). 그런데 휴대폰 실명제는 이러한 국가의 헌법적 의무에 반하는 제도입니다.

특히 부정가입방지시스템의 구축·운영 등의 업무를 기업들로 이루어진 민간단체인 한국정보통신진흥협회에 위탁하고 있는 것은 더욱 무책임한 처사라 하지 않을 수 없습니다. 게다가 방송통신위원회와 이동통신 3사는 본인확인을 위해 작년말부터 신분증 스캐너를 전면 도입해 운영하고 있는데, 실효성이 없을 뿐만 아니라 정보 유출의 위험성만 높아진 상황입니다(첨부자료 3. 2016. 11. 23.자 지디넷코리아 기사). 또한 개인정보보호법제의 개정으로 주민등록번호의 수집이 원칙적으로 금지되었지만, 휴대폰 실명제에 의해 주민등록번호와 연계된 휴대폰이 본인확인 및 인증 수단으로 널리 활용되고 있어 개정의 취지를 무색하게 하고 있습니다.

이렇듯 휴대폰 실명제는 개인정보의 과도한 집적으로 해킹 등을 통한 유출 위험성을 높입니다. 헌법재판소도 실명제 하에서 '개인정보의 집적 및 유출 위험성'이 점증한다고 확인한 바 있습니다(헌재 2012. 8. 23. 2010헌마47, 252(병합)).

(4) 통신자료제공 제도의 남용

전기통신사업법 제83조 제3항은 수사기관이 영장 없이 전기통신사업자에게 이용자의 개인정보를 요청할 수 있는 '통신자료제공' 제도를 규정하고 있습니다. 그런데 최신 통계를 보면 통신자료 제공의 대부분이 이통사에 의해 이루어지고 있습니다(첨부서류 4. 16년 하반기 통신자료 및 통신사실확인자료 제공 등 현황).

(단위 : 문서수)

구 분	'15년		'16년	
	상반기	하반기	상반기	하반기
유선전화	65,970	65,410	65,075	58,177
이동전화	441,799	451,152	463,444	438,616
인터넷 등	52,258	48,385	46,250	38,052
합 계	560,027	564,847	574,769	534,845

원칙적으로 수사기관의 개인정보 취득은 국민의 기본권에 대한 제한이므로 헌법상 영장주의 원칙이 적용됩니다. 하지만 그동안 수사기관은 영장주의를 우회하는 방법으로 통신자료제공 제도를 남용해 왔습니다. 특히 이통사의 경우 수사기관의 제공 요청을 거절하는 경우가 거의 없었기에, 전 국민이 통신자료제공 제도에 의해 위법하게 개인정보자기결정권을 침해받았다고 해도 과언이 아닙니다. 이렇듯 위헌적인 통신자료제공 제도의 남용이 가능한 이유는 휴대폰 실명제 내지 본인확인제로 인해 이통사가 이용자의 개인정보를 수집·보관하고 있기 때문입니다.

통신자료제공 제도를 개선 내지 폐지하기 위해 수많은 법안이 발의되어 있으며, 국회 입법조사처는 특히 우리나라의 특수한 통신환경에서는 주민등록번호 등과 같은 개인 식별정보의 범용적 활용이 입법적으로 제도화되어있어 범죄수사 등 공익적 필요성을 넘어서서 당해 이용자의 사생활의 상당부분을 추적하는 것까지 가능하여 이용자들의 기본권 보장의 문제를 더욱 면밀하게 검토할 필요가 있다고 보아, 통신자료 제공요청에 대한 실효적인 사전 및 사후 통제 방안이 필요하다고 제언한 바 있습니다(첨부서류 5. 프라이버시 보호를 위한 통신자료 제공제도의 개선방향 참조).

마. 소결

위와 같이 이 사건 본인확인 의무 조항은 수단의 적합성, 침해의 최소성, 그리고 법익의 균형성을 갖추지 못하였기에 과잉금지의 원칙에 위반하여 청구인들의 익명 통신의 자유, 사생활의 비밀과 자유 그리고 개인정보자기결정권을 침해하고 있습니다.

IV. 결론

이상과 같이 이 사건 본인확인 의무 조항은 청구인들의 익명 통신의 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 침해하여 헌법에 위반되므로 위헌 결정을 내려주시기 바랍니다.

첨 부 서 류

1. 유엔 의사표현의 자유 특별보고관 헌재 의견서
2. 2017. 9. 27.자 뉴스1 기사
3. 2016. 11. 23.자 지디넷코리아 기사
4. 16년 하반기 통신자료 및 통신사실확인자료 제공 등 현황
5. 프라이버시 보호를 위한 통신자료 제공제도의 개선방향

2017. 11.

위 청구인들의 대리인

변호사 김 가 연

헌법재판소 귀 중

대한민국 헌법재판소

2016 헌마 388

유엔 의사·표현의 자유특별보고관 데이비드 케이의 제 3자 의견서

데이비드 케이 (David Kaye)
유엔 의사·표현의 자유 특별보고관
미국 캘리포니아 대학교 어바인 로스쿨
국제사법클리닉,
법학교수 및 소장
전화번호: (949) 824-2427
주소: 401 East Peltason Dr. Ste. 3800-C
Irvine, CA 92697-8000
홈페이지: https://freedex.org/

2017. 5. 9.

목차

I. 서론

1. 의사표현의 자유에 관한 유엔 특별보고관 데이비드 케이(David Kaye, 이하 "본인"이라고 합니다)는 대한민국 헌법재판소에 법정조언자(*amicus curiae*)로서 이 의견서를 제출합니다.[1] 귀 재판소에서 심리중인 2016 헌마 388 통신자료취득행위 위헌확인 등 사건은 전기통신사업법 제 83 조 제 3 항 및 제 4 항에 관한 것입니다.

2. 이 의견서를 비롯하여, 유엔 특별보고관의 의견서 제출은 자발적으로 이루어지는 것이고, 이러한 의견서 제출은 '1946 년 유엔 특권 및 면제에 관한 협약' 상 유엔 및 그 직원, 임무수행 중인 전문가의 특권 및 면제에 대한 명시적 또는 묵시적 포기로 간주되지 않습니다. 유엔 특별보고관의 입장 및 견해는 그의 독립성에 의한 것으로서, 이것은 유엔, 유엔 인권 이사회, 유엔 인권최고대표사무소 및 그 관계자들의 견해가 아닙니다.

II. 이 사건에 대한 유엔 특별보고관의 이해관계

3. 대한민국이 1990. 4. 10. 비준한 '시민적·정치적 권리에 관한 국제규약'(The International Covenant on Civil and Political Rights, 이하 "규약"이라고 합니다)에서는, 의사의 자유(규약 제 19 조 제 1 항)와 표현의 자유(규약 제 19 조 제 2 항)를 보장해야 할 당사국의 의무를 규정하고 있습니다. 유엔의 핵심 인권 기구인 유엔 인권이사회에서는 의사표현의 자유가 "인권과 자유의 향유에 있어 본질적인 것이며, 민주주의 사회의 건설 및 강화를 위한 근간을 이룬다"라고 천명하였습니다.[2] 대한민국은 위 규약의 당사국으로서 "최선의 노력을 다하여" 이러한 의무를

[1] The Special Rapporteur would like to thank Mr. Calvin Bryne, Ms. Sarah Choi, and Mr. Adam Lhedmat, student advocates with the University of California Irvine School of Law International Justice Clinic, and Mr. Amos Toh, legal advisor to the mandate and Ford Foundation Fellow, for their assistance with the preparation of the brief.

[2] Human Rights Council Res. 23/L.5, at ¶2, U.N. Doc. A/HRC/23/L.5 (April 9, 2014).

준수해야 하며, "국내법 규정을 근거로 이러한 규약상 의무 위반을 정당화" 할 수는 없습니다.[3]

4. 유엔 인권이사회 결의안 7/36, 3(c)에서는, "모든 방식의 의사표현의 자유를 보다 증진시키고 보호할 수 있는 방안에 대하여 권고"할 수 있도록 본인에게 권한을 위임하였습니다.[4] 위와 같은 위임에 의하여 이루어지는 이 의견서 상 권고는 국제인권법의 분석에 기초하고 있으며, 여기에는 관련 법제, 기준, 국제 실무뿐 아니라 관련 지역 및 국내법, 기준 및 실무 분석도 포함하고 있습니다. 이 사건에서 문제가 되고 있는 전기통신사업법 제 83 조 제 3 항 및 제 4 항의 규정은 국제인권법과의 합치, 의사표현의 자유에 관한 궁극적인 권리의 침해수준과 관련하여 중대한 문제를 야기하고 있습니다.

5. 앞서 말한 권한에 근거하여, 본인은 온라인 상 표현의 자유에 대한 위협이 현저하게 증가하고 있음을 주시해왔습니다. 전임 유엔 특별보고관과 본인은 이러한 위협들 중에서도 온라인 상 암호화 해제, 익명성 훼손을 목적으로 무분별하고 공격적으로 이루어지는 통신감시 및 시도들이 확대되고 있음을 보고해왔습니다.[5] 그런데 이 사건 역시 이와 비슷한 우려를 야기하고 있습니다.

III. 대한민국은 국가기관의 이용자 정보 취득이 규약 제 19 조 제 1 항 상의 의사의 자유를 침해하지 않도록 보장해야 합니다.

6. 규약 제 19 조 제 1 항은 "모든 사람은 어떠한 간섭 없이 스스로 의사(의견)를 가질 권리가 있다"라고 규정하고 있습니다. 표현의 자유에 대하여는 규약 제 19 조 제 3 항

[3] Vienna Convention on the Law of Treaties arts. 26-27, May 23, 1969 1155 U.N.T.S. 331.

[4] Human Rights Council Res. 7/36 at ¶3(c), U.N. Doc. A/HRC/7/36 (Mar. 28, 2008).

[5] See e.g. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) ("2013 Report"); Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, (May 22, 2015) ("2015 Report"); Human Rights Council Res. 34/7 (Mar. 22, 2017).

상의 구체적인 기준에 의거하여 "법률 또는 다른 권한에 의해 제한"될 수 있음을 규정하고 있는 반면, 의사의 자유에 대하여는 "절대적 보장"으로 규정하고 있습니다.[6] 의사를 가질 권리는 인간의 존엄성과 민주적 자치를 위한 근본적인 요건이며, 위 규약에서 이에 대한 어떠한 간섭, 제한 또는 제재를 허용하지 않을 정도로 중대한 보장에 해당하는 것입니다.[7]

7. 유엔 인권이사회, 유엔 총회, 유럽 평의회를 비롯한 다수의 국제 및 지역 기구들은 온라인뿐만 아니라 오프라인 상에서도 의사표현의 자유를 동등하게 보장해야 한다고 결론을 내렸습니다.[8] 의사의 자유를 침해하는 오프라인 상 간섭행위의 예로는 신체적 학대, 구금, 기타 경미한 처벌을 들 수 있습니다.[9] 요즘 같은 디지털 시대에서 개인들은 온라인 상 "하드 드라이브, 클라우드(cloud), 전자메일 보관함 등에 자신의 견해, 검색결과, 열람내역을 저장"합니다.[10] 이러한 디지털 플랫폼(digital platforms)은 각 개인들이 "의견을 형성하고 추론을 통해 발전"시킬 수 있게 해줍니다.[11] 따라서 전기통신사업법 제 83 조 제 3 항 및 제 4 항을 근거로 국가기관이 그러한 정보를 취득함에 있어서, 그것이 개인의 의사 형성 및 보유의 권리를 침해하는 방식으로 이루어져서는 안 됩니다.

IV. 규약 제 19 조 제 2 항 및 제 3 항에 의하여, 대한민국은 국가기관이 이용자 정보를 취득하는 것이 익명 표현 및 통신의 자유를 과도하게 침해하지 않도록 보장하여야 합니다.

[6] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary*, at 441 (Feb., 1993).

[7] 2015 Report at ¶19 (May 22, 2015).

[8] See, e.g. G.A. Res. 68/167 (Jan. 21, 2014); Human Rights Council Res. 26/13 (July 14, 2014); and Council of Europe CM/Rec(2014)6 (Apr. 16, 2014).

[9] *See Yong-Joo Kang v. Republic of Korea*, Communication No. 878/1999, U.N. Doc. CCPR/C/78//D/878/1999, at ¶¶ 2.5, 7.2, and 7.3 (July 15, 2003).

[10] 2015 Report, at ¶20 (May 22, 2015).

[11] Nowak, *supra* at 441 (emphasis added).

A. 익명 표현은 규약 제 19 조 제 2 항에 의하여 보장되는 표현의 자유를 행사하는 방식입니다.

8. 규약 제 19 조 제 2 항은 다음과 같이 규정하고 있습니다.

> "모든 사람은 표현의 자유를 가진다. 이러한 권리는 국경을 불문하고 모든 종류의 정보와 아이디어를 구두, 서면 또는 인쇄물, 예술의 형태 또는 자신이 선택한 매체를 통하여 찾고, 받고, 전달할 수 있는 자유를 포함한다."

9. 위 규약은 익명성에 대하여 명시적으로 언급하고 있지는 않습니다. 그러나 규약 제 19 조에 대한 입안과정을 보면, 입안자들이 익명성을 표현의 자유에 있어서 중요한 것으로 보았음을 알 수 있습니다. 이러한 논의과정 중에서 당사국들은 규약 제 19 조 제 1 항에 "익명성은 허용되지 않는다"라는 문구를 추가하는 방안에 반대하였는데, 이는 "저자를 보호하기 위해 익명성이 필요할 수 있다", "그러한 익명성 불허 문구는 필명 사용을 제한할 수 있다"라는 점을 고려한 것입니다.[12]

10. 당사국들의 위와 같은 고려는 익명성이 사회 및 정치 담론에의 국민 참여에 있어서 필수적일 수 있음을 보여줍니다. 필명(개인이 통신 또는 업무상 실명 대신 사용하는 가명)은 그들이 실제 정체를 드러낼 때 보다 더 많은 아이디어와 견해들을 탐구하고 전달할 수 있도록 보호하는 기능을 합니다.[13] 특히, 개인들은 그들에게 가해질 수 있는 사회적 낙인, 학대, 신체 안전에 대한 위협 때문에 드러내지 못하는 비전형, 비주류 또는 소수의 의견에 대해 표현하고 토론하고자 할 수 있습니다.

11. 디지털 상의 "필명" 또한 규약 제 19 조 제 2 항에 의하여 동등하게 보장됩니다. 블로그, 소셜 미디어 플랫폼(social media platforms), 온라인 토론장, 사적인 연락 등에서 많은 인터넷 이용자들은 익명성을 위하여 온라인상 가명을 사용하고 있습니다. 그들은

[12] Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights*, at 379-80 (Feb. 17, 1987).

[13] 2015 Report, at ¶9 (May 22, 2015).

자신들의 신상을 좀 더 효과적으로 숨기기 위하여 가상 사설망(VPNs), 프록시 서비스(proxy services), 익명 네트워크 및 소프트웨어, P2P 네트워크와 같은 암호 및 익명화 도구를 혼합하여 사용할 수도 있습니다.[14]

12. 규약 제 19 조 제 2 항은 이러한 기술발전에도 적용이 가능하도록, 넓은 범위에서 초안이 작성되었습니다. 위 규정 상 보호기준은 개인이 자신을 표현하기로 선택한 위치 또는 방법에 관계없이 모두 적용됩니다. 이를 위하여 당사국들은 그 당시 현존하는 매체를 열거하는 대신, "자신이 선택한 매체를 통하여"라는 일반적인 문구를 사용하기로 결정하였습니다.[15] 이러한 결정은 권리가 온라인 및 오프라인 상에서 동등하게 보호되어야 한다는 국제적인 합의와 일맥상통합니다.[16] 그러므로 익명표현은 온라인 또는 오프라인에 상관 없이 "어떠한 매체를 통해서라도" 보호되는 것입니다.

13. 익명 통신은 그것 자체로서 규약 제 19 조 제 2 항에 의하여 보호되는 표현 활동이 될 수 있습니다. 현대 문화에서 가이포크스(Guy Fawkes) 마스크 착용은 시위에 참여하는 자의 정체를 숨기고 정치적인 진술을 하게 하는 두 가지 기능을 모두 수행합니다.[17] 즉, 자신의 정체를 숨기는 행위 자체가 의사표현의 한 형태일 수 있습니다.

B. 익명으로 통신할 수 있는 권리는 규약 제 19 조 제 2 항 상 표현의 자유를 실현하기 위해 필요한 사생활의 자유 영역을 창출합니다.

[14] *Id*.

[15] 2015 Report, at ¶26 (May 22, 2015).

[16] *Supra* note 8.

[17] *See, e.g.*, Glenda Kwek, *V for vague: Occupy Sydney's faceless leaders*, The Sydney Morning Herald, (Oct. 14, 2011), available at: http://www.smh.com.au/nsw/v-for-vague-occupy-sydneys-faceless-leaders-20111014-1loy6.html.

14. 규약 제 17 조에 의하면, 모든 사람은 "자신의 사생활의 자유, 가족, 가정 또는 서신에 대한 임의적이고 불법적인 간섭"으로부터 "법에 의한 보호를 받을 권리"를 가집니다. 유엔 총회, 유엔 인권이사회, 유럽 평의회, 미주 인권위원회를 비롯한 많은 국제 및 지역기구들은 사생활의 자유 보호가 표현의 자유의 행사에 있어서 중요하다는 점을 확인하였습니다.[18] 사생활의 자유에 대한 과도한 침해는 결과적으로 "아이디어의 자유로운 발전 및 전달을 직접 또는 간접적으로 제한"할 수 있습니다.[19]

15. 온라인상 익명성은 이러한 권리들 간의 밀접한 관련을 보여주며, "임의적이고 불법적인 간섭 또는 공격 없이 의견 개진 및 표현의 자유를 행사할 수 있는 사생활의 자유 영역"을 만듭니다.[20] 특히, 암호화 및 익명화 도구들은 전자메일, 문자메세지, 채팅 어플리케이션, 기타 온라인상 연락 등 온라인 통신 상의 사생활의 자유를 보호하며, 이로써 이러한 온라인 통신은 의견 형성 및 공유에 있어서 대중적인 매체가 되었습니다.[21] 이와 반대로, 익명에 대한 제한은 자기 검열을 강화시킬 수 있습니다. 예를 들어, 전임 유엔 특별보고관은 의사소통 상의 익명성 배제는 "보복의 두려움 때문에 신고하기를 꺼려하는 폭력 및 학대의 피해자들에게 명백한 위축효과를 가져온다"는 사실을 발견하였습니다.[22]

16. 이용자가 전기통신사업자에게 자신의 개인정보를 공개하는 경우라고 하더라도, 이것이 개인의 익명 표현 및 통신의 자유를 존중하고 보장해야 할 국가의 의무를

[18] 2013 Report, at ¶24 (Apr. 17, 2013); *see also* G.A. Res. 68/167 (Jan. 21, 2014); Human Rights Council Res. 34/7 (Mar. 22, 2017); 2015 Report, at ¶16 (May 22, 2015); The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶19 (Apr. 17, 2013); Freedom of Expression and the Internet, Inter-American Commission for H.R., Office of the Special Rapporteur for Freedom of Expression, at ¶¶ 130, 150 (Dec. 31, 2013); The Rule of Law on the Internet and in the Wider Digital World, Council of Europe, Commissioner for Human Rights, at ¶88 (Dec. 8, 2014); Declaration on freedom of Communication on the Internet, Council of Europe, at principle 7 (May 28, 2003).

[19] 2013 Report, at ¶24 (Apr. 17, 2013).

[20] 2015 Report, at ¶16 (May 22, 2015).

[21] *Id.* at ¶17.

[22] 2013 Report, at ¶24 (Apr. 17, 2013).

면제하는 것은 아닙니다. 익명은 비밀이 아닙니다. 익명은 개인이 어떤 상황 하에서 누구에게, 어떤 목적으로 자신의 정체를 공개할지 여부를 결정할 권한에 대한 것입니다. 이와 비슷한 취지로 유럽인권재판소에서는 "민주사회 하에서 정당화되지 않는 한 바람직하지 않고 불법"이라고 본 통신 비밀 침해행위(the interception of communications)와 전화통신사업자에 의한 미터링("metering" 즉, 통신 메타데이터 수집)을 구분하여 판단하였습니다.[23] 이와 같이, 통신 이용자들은 인터넷 또는 통신 서비스를 이용하기 위하여 자신의 개인정보를 전기통신사업자에게 공개(또는 수집을 허락)할 수 있으나, 이것이 국가기관 또는 제 3 자에게 해당 정보에 대한 자유로운 접근을 허용하는 것은 아닙니다. 이용자들은 법적 절차적 보호를 통하여 법 집행기관 및 다른 국가기관으로부터 익명으로 남을 수 있습니다.

C. 전기통신사업법 제 83 조 제 3 항 및 제 4 항에 의한 전기통신사업자의 통신자료 제공 및 국가기관의 취득은, 규약 제 19 조 제 2 항에서 보호하는 익명 표현 및 통신의 자유를 침해합니다.

17. 법 제 83 조 제 3 항은 다음과 같이 규정합니다.

"전기통신사업자는 법원, 검사 또는 수사관서의 장, 정보수사기관의 장이 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출을 요청하면 그 요청에 따를 수 있다."

1. 이용자의 성명
2. 이용자의 주민등록번호
3. 이용자의 주소
4. 이용자의 전화번호
5. 이용자의 아이디(컴퓨터시스템이나 통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호를 말한다)

[23] Malone v. United Kingdom, App. No. 8691/79, Judgment, 82 Eur. Ct. H.R. 10, ¶84.

6. 이용자의 가입일 또는 해지일

18. 법 제 83 조 제 4 항은 다음과 같이 규정합니다.

> "제 3 항에 따른 통신자료제공 요청은 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있을 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 해소되면 지체 없이 전기통신사업자에게 자료제공요청서를 제출하여야 한다."

19. 법 제 83 조 제 3 항 및 제 4 항에 의한 국가기관의 통신자료 취득은 익명 표현과 통신의 자유를 잠재적으로 제한합니다. 법 제 83 조 제 3 항에 의해 요청 가능한 정보의 범위는 개인의 성명, 주소 및 근무지, 전화번호, 이메일 주소 및 이용자 아이디까지 포함하고 있으며, 이는 법 집행기관, 정보수사기관 및 다른 국가기관로 하여금 온라인 및 오프라인 상 정체를 광범위하게 볼 수 있는 권한을 부여하고 있습니다. 위와 같은 정보들은 다른 인터넷 및 인터넷 IP 주소, 셀사이트 위치정보, 전화번호, 통화 및 이메일의 날짜 및 시간과 같은 통신 메타데이터와 결합되거나 분석될 수 있으며, 이는 "사적 통신 내용에 의하여 전달되는 것 이상의 개인의 행동, 사회적 관계, 개인의 취향과 정체성"을 보다 구체적으로 그려낼 수 있게 합니다.[24]

20. 국가기관의 잠재적인 정보 취득 범위를 감안하면, 일반적인 온라인 상 익명은 "피상적이고 쉽게 침해될" 수 있는 것입니다.[25] 예를 들어, 가명 또는 암호화 도구들(기본적으로 웹 트래픽을 암호화하는 HTTPS 웹사이트)로는 충분하지 않을 수 있습니다. 개인정보의 공개를 피하고자 하는 이용자들, 특히 소수의견을 표현하거나 공익을 위하여 민감한 정보를 공개하고자 하는 자들은 기술적으로 복잡하고 사용하기

[24] The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶19 (Apr. 17, 2013).

[25] 2015 Report, at ¶9 (May 22, 2015)

어려운 익명화 소프트웨어 및 도구를 사용할 수 밖에 없을 것입니다. 이러한 어려움 또는 위험 때문에 많은 이들이 말하는 것 자체를 포기할 수도 있습니다.

21. 이용자 정보에 대한 국가기관의 접근가능성만으로도 개인이 자신을 자유롭게 표현하는 것을 방해할 수 있습니다. 즉, 국가기관이 개인정보에 대하여 접근할 수 있는 법적 체제의 존재만으로도 "표현과 결사의 자유를 포함하여 권리 전반에 대한 잠재적인 위축효과를 가져오며, 사생활의 자유의 침해를 발생"시킬 수 있습니다.[26] 이러한 위축효과는 변호인과 의뢰인의 관계, 언론인과 정보원, 내부고발자, 인권활동가, 소수 및 취약 집단에게 불리한 결과를 가져올 수 있습니다.

D. 규약 제 19 조 제 3 항은 국가기관의 개인정보 취득은 법에 의하여, 합법적인 목표를 달성하기 위해 필요한 최소한의 수준에서 이루어질 것을 요구합니다.

22. 규약 제 19 조 제 3 항은 다음과 같이 규정합니다.

> "규약 제 19 조 제 2 항에서 규정하고 있는 권리의 행사는 특별한 의무와 책임이 따른다. 이러한 권리는 제한이 될 수 있으나, 그와 같은 제한은 법이 정하는 바에 따라 필요한 경우에만 가능하다."
>
> (a) 다른 이들의 권리 또는 명예를 존중하기 위하여
>
> (b) 국가 안보 또는 공공질서, 공중 보건 및 윤리의 보호를 위하여[27]

23. 위 규약의 이행을 감시하는 유엔 인권위원회에서는, 표현의 자유에 대한 규제가 "법이 정하는 바에 따라" 이루어지기 위해서는 그러한 규제가 명확하여야 하고, 공개적이고 투명해야 하며, 국가기관에게 그러한 규제를 적용할 수 있는 무제한의

[26] The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶20 (Apr. 17, 2013).

[27] International Covenant on Civil and Political Rights art. 19(3), Dec. 16, 1966, 999 U.N.T.S. 171 (emphasis added).

재량권을 부여하는 것을 피해야 한다고 하였습니다.[28] 따라서 국가기관의 이용자 정보 취득 조건에 관한 법률 및 규정에는 "개인이 사전 통보를 받고 그 결과를 예견할 수 있도록 명확한 기준"을 정해야 합니다.[29] 통신상 감시행위와 관련하여, 정부는 이용자 정보에 대한 접근이 표현의 자유를 제한하는 무분별한 재량권을 갖는 것은 아니라는 점도 입증하여야 합니다.

24. 이용자 정보를 취득하는 국가기관의 권한 범위는 규약 제 19 조 제 3 항에서 정한 법 집행, 국가 안보, 공공안전의 목적 달성을 위해 "필요한" 정도에 한하여 이루어져야 합니다. 여기에서 필요성은 그 제한이 단순히 합리적이고 유용하며 바람직한 것 이상이어야 함을 의미합니다.[30] 국가는 "구체적이고 개별적으로 위협의 정확한 성격"과 그 위협과 취득 정보의 범위 및 그 취득방법 사이의 "직접적이고 긴밀한 관계"를 입증해야 합니다.[31] 국가 안보의 관점에서, 전임 유엔 특별보고관은 정보 취득 목적을 광범위하게 정의하는 것은 "인권운동가, 언론인 또는 활동가와 같은 취약 집단을 겨냥한 조치들을 정당화하는 수단으로서 국가정부에 의한 조작활동을 용이하게" 한다는 사실을 발견하였습니다.[32]

25. 또한 '필요성'은 국가기관의 이용자 정보 취득 권한에 대한 비례성 판단을 보여주는 것입니다.[33] 유엔 인권위원회는 비례성 판단을 통하여 그러한 정보 취득행위가 "보호 기능을 달성할 수 있는 방법 중 가장 침해가 적은" 것임을 보장해야 한다고 했습니다.[34] 다시 말해, 이용자 정보 취득은 침해의 정도가 경미한 다른 감시 또는 조사방법이

[28] U.N Doc. CCPR/C/GC/34, at ¶39 (Sep. 12, 2011); 2015 Report, at ¶32 (May 22, 2015).

[29] 2013 Report, at ¶83 (Apr. 17, 2013).

[30] 2015 report, at ¶34 (May 22, 2015)

[31] U.N Doc. CCPR/C/GC/34, at ¶35.

[32] 2013 Report, at ¶60 (Apr. 17, 2013).

[33] U.N Doc. CCPR/C/GC/34, at ¶34 (Sep. 12, 2011); *See also* Lohe Issa Konate v. Burkina Faso, No. 004/2013, Afr. Ct. H.P.R., at ¶¶ 148, 149 (Dec 5, 2014); The Sunday Times v. The United Kingdom, No. 6538/74, Eur. Ct. H.R. at ¶¶ 59, 62 (Apr. 26, 1979).

[34] *Id*.

존재하지 않는 경우에만 이루어져야 합니다. 투명하고 철저한 공적 검토가 가능하게 하기 위해서는 그러한 정보취득에 대한 "구체적이고도 근거가 있는 공적 확인"이 중요합니다.[35]

V. 영장 제공 없이 이용자 정보를 요청하는 것은, 익명 표현 및 통신의 자유를 침해하지 않아야 할 대한민국의 의무에 반하는 것입니다.

26. 국가기관이 사전 영장 제시 없이 이용자 정보를 요구하는 것은 앞서 말한 적법성, 필요성 및 비례성의 원칙에 반합니다. 그러한 요구는 오로지 충분한 법적 기준과 합법적이고 공정한 사법 기구의 명령에 의하여, 법적 목표 달성을 위한 필요성 및 비례성을 판단한 후에 부여되어야 합니다. 본인의 관련 국제 법제 및 실무에 대한 분석결과를 통하여, 이러한 견해가 관련 국제 및 지역기구 및 여러 국가들의 공통된 의견임을 알 수 있었습니다.

A. 영장주의에 의하지 않은 이용자 정보 요구는, 국가기관의 개인정보 취득이 사법 명령에 의하여 승인되어야 한다는 국제적인 합의와 일치하지 않습니다.

27. 유엔 기구들은 고객정보 및 통신 메타데이터 등 개인정보에 대한 국가기관의 요구가 합법적이고 독립적이며 공정한 사법절차에 의해 규제되어야 한다고 결론을 내렸습니다. 2014 년 유엔 총회에서 회원국들에게 "국가 통신 감시"와 "개인 데이터 수집"에 있어서 "투명성을 보장 할 수 있는 독립적이며 효율적인 기존의 국내 감독 체제를 적절하게 유지하고 책임지도록" 촉구했습니다.[36] 유엔 총회를 통해 통신 감시가 인권에 미치는 영향에 대해 의견을 제안하도록 위임 받은 유엔 인권 고등판무관은, "독립성, 공정성 및 투명성에 관한 국제 기준에 부합하는 사법적 관여는, 전반적인 법정 제도가 국제 인권법에서 요구하는 최소한의 기준에 도달할 수 있도록

[35] *See* G.A. Res. 69/397, ¶12 (Sep. 23, 2014).

[36] G.A. Res. 69/166 (Feb. 10, 2015) at ¶4(d) (emphasis added).

할 것이다"라고 강조하였습니다.[37] 2016 년 유엔 총회에서 이와 유사한 권고안을 채택하면서, 회원국들에게 "개인정보 수집과 관련하여 투명성과 책임을 보장할 수 있는, 독립적이고 효율적이며 능력 있는 공정한 사법, 행정, 및 입법 상 국내 감독 기구를 창설 또는 유지"할 것을 요구하였습니다.[38]

28. 표현의 자유에 관한 국제 및 지역 전문가들도 사법 절차의 필요성에 대하여 재차 확인하였습니다. 2013 년 표현의 자유 및 인터넷에 관한 연구에서, 미주 인권위원회의 특별보고관실은 "통신 비밀 침해행위를 승인하는 법률에서는 정부가 그러한 행위를 하고자 하는 이유를 투명하고 구체적으로 규정해야 하며, 이는 오로지 판사에 의하여 승인되어야 한다"라고 결론 내렸습니다.[39] 마찬가지로, 전임 유엔 특별보고관은 인권법에 따라 "국가기관에 대한 통신자료 제공은 법원 또는 감독기관와 같은 독립적인 기구에 의하여 감시되어야 한다"고 밝혔습니다.[40] 두 특별보고관 모두 2013 년 '감시 체제가 표현의 자유에 미치는 영향에 관한 공동 선언'에서 이러한 권고를 되풀이하였으며, 국가들로 하여금 "개인정보의 수집은 독립적인 감독 기구에 의하여 감시되어야 하며, 충분한 적법 절차 보장 및 사법 감독에 의하여 관리"할 것을 국가들에게 촉구하였습니다.[41]

---

[37] The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶38 (Apr. 17, 2013) (emphasis added).

[38] G.A. Res. 71/39, at ¶5(d) (Nov. 16, 2016) (emphasis added).

[39] *Freedom of Expression and the Internet*, Office of the Special Rapporteur for Freedom of Expression, Inter-American Commission for Human Rights, at 156 (Dec 31, 2013), available at: https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf, (emphasis added).

[40] 2013 Report, at ¶86 (Apr. 17, 2013) (emphasis added).

[41] *Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression*, United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression; Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, available at: https://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

29. 관련 지역 및 국내의 법제 조사결과 또한 사법적 사전 승인절차가 국가기관의 불법적이고 부적절한 개인정보 수집에 대한 중요한 보호장치가 되어준다는 사실을 보여줍니다. 전기통신사업법 제 83 조 제 3 항 및 제 4 항과 유사한 규정에 대해 다룬 R v. Spencer 사건에서, 캐나다연방대법원은 제 3 의 운영자에 의해 관리되는 가입자 정보를 아무런 영장제시 없이 요구하는 법 집행은 위헌이며, 설사 그러한 요구가 구속력이 없는데도 운영자가 자발적으로 해당 정보를 공개하였다고 하더라도 이와 같다는 취지로 판시하였습니다.[42] 위 법원은 그 근거로서 "이러한 정보의 공개는 주로 온라인상에서 사적이고 민감한 활동을 하는 이용자의 신원확인으로 이루어지며, 이러한 해당 활동들이 익명 하에 이루어진 점을 전제로 하는 것입니다"라고 하였습니다. [43] 따라서 "경찰이 인터넷서비스 운영자에게 자발적으로 정보를 공개하라고 요구하는 것은 수사에 해당"하고, 이는 영장주의와 같은 적법절차의 승인에 의하여 이루어져야 합니다.[44]

30. 유럽사법재판소는 2014 년 *Digital Rights Ireland and Seitlinger* 판결에서 EU 데이터 보존지침(EU Data Retention Directive)에 사법 사전승인 절차가 없음을 이유로 위 지침을 무효화하기에 이르렀습니다. 특히 위 재판소는 위 지침에 의거하여 통신사업자가 보유한 개인정보의 국가기관 취득과 관련하여, 그러한 정보취득은 "법원 또는 독립 행정 기구를 통한 사전 승인에 의하여 목표 달성에 필요한 범위"로 제한된 것이 아니라고 판시하였습니다. [45] 이와 마찬가지로, 멕시코 연방 대법원은 영장 없이 휴대전화 메타데이터에 대해 법을 집행한 것은 통신자의 사생활의 자유를 침해한다고 결정하였습니다.[46]

---

[42] *See R v. Spencer*, 2 S.C.R. 212 (June 13, 2014).

[43] *Id.* at ¶66.

[44] *Id.*

[45] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine, and Natural Resources*, E.C.J. 238 at ¶62 (Apr. 8, 2014)

[46] *See Contradicción de Tesis*, 2012 Mex. S.C. 194, (Oct. 10, 2012).

31. 또한 관련 각국 입법 구조 조사 결과 12 개국 이상의 나라들이 이용자 정보 취득을 위해서는 영장 또는 다른 형식의 사법 절차를 요구한다는 것을 발견하였습니다.[47] 아제르바이잔, 체코, 덴마크, 모리셔스, 루마니아, 우크라이나 및 미국 등 다양한 국가에서는 여러 단계의 사법 사전승인이 이루어지고 있습니다.[48] 스페인, 프랑스 및 일본에서도 요청된 정보가 통신의 비밀에 영향을 미치는 경우 법적 사전 승인절차가 필요합니다.[49]

32. 마지막으로, 귀 재판소는 온라인 상 익명표현에 대한 규제 제한이 중요하다고 보고 있습니다. 헌법재판소 2012. 8. 23. 선고 2010 헌마 47, 252(병합) 정보통신망이용촉진및정보보호등에관한법률 제 44 조의 5 제 1 항 제 2 호 등 위헌확인 사건에서 귀 재판소는 다음과 같이 판시하였습니다.

> 인터넷 공간에서 이루어지는 익명표현은 인터넷이 가지는 정보전달의 신속성 및 상호성과 결합하여 현실 공간에서의 경제력이나 권력에 의한 위계구조를 극복하여 계층·지위·나이·성 등으로부터 자유로운 여론을 형성함으로써 다양한 계층의 국민 의사를 평등하게 반영하여 민주주의가 더욱 발전되게 한다. 따라서 비록 인터넷 공간에서의 익명표현이 부작용을 초래할 우려가 있다 하더라도 그것이 갖는 헌법적 가치에 비추어 강하게 보호되어야 한다.[50]

33. 개인정보 취득에 대한 영장주의를 인정하는 것은 이러한 우려들에 대한 심사숙고이며, 그러한 결정은 귀 재판소의 결정이 국제적인 합의와 일치되게 할 것입니다.

B. 영장주의는 대한민국 정부의 이용자 정보에 관한 불필요하고 부적절한 긴급요구를 제한할 것입니다.

---

[47] *Rules on obtaining subscriber information*, Cybercrime Convention Committee, T-CY(2014), at 17 (Dec. 3, 2014).

[48] *Id.*

[49] *Id.*

[50] Const. Ct., 2010 Hun-Ma 47, 252 (Aug. 28, 2012) (S. Kor.).

34. 사실 몇몇 국가들은 영장제시 없이 이용자 정보를 취득하면서 그들의 인권 의무사항을 잠재적으로 위반하고 있습니다.[51] 예를 들어, 호주와 불가리아의 고위공무원은 "경찰의 형식적 요청서"에 의하여 이용자 개인정보를 취득할 수 있습니다.[52] 그러나 본인의 견해로는, 대한민국에서는 이미 국가기관이 이용자 정보를 많이 요구하고 있으며 이로 인해 이용자의 표현의 자유에 대한 위험이 악화되고 있으므로, 위 국가들과 같은 구조가 반영되어서는 안 된다고 봅니다.

35. 이와 비슷한 전 세계적인 상황을 조사한 바에 따르면, 대한민국의 1 인당 국가기관의 이용자 정보 요구 건수가 가장 높았습니다. 2011 년에는 인구가 5 천만명이 조금 못 미치는데 개인정보 취득 건수는 584 만건을 기록하였고, 이는 9 명 당 1 건의 요청이 있는 것으로서 굉장히 높은 비율이었습니다. 2015 년의 요청 건수는 대략 10 억 건으로 현저히 증가했습니다.[53]

36. 이러한 수치는 다른 민주주의 국가의 수치에 비해서 상당히 높은 것입니다. 약 6,500 만명의 인구를 가진 영국에서는, 2015 년에 761,702 개 통신자료 항목이 제공 승인되었고, 이 중 절반은 고객 개인정보였습니다. 이는 85 명에 대한 1 개 통신자료 항목 및 170 명에 대한 1 개 통신자료 항목의 평균비율입니다.[54] 프랑스에서는 2015 년

---

[51] *Rules on obtaining subscriber information*, Cybercrime Convention Committee, T-CY(2014), at 16 (Dec. 3, 2014).

[52] *Id.*

[53] *See 2016 First Semi-Annual Numbers of Communication Data Disclosures and Communication Metadata Acquisitions*, Ministry of Science, ICT and Future Planning (November 1, 2016), available at: http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1316113&snsMId=NzM%3D&getServerPort=80&sn.sLinkUrl=%2Fweb%2FmsipContents%2FsnsView.do&getServerName=www.msip.go.kr.

[54] Each item of data is "a request for data on a single identifier or other descriptor, for example, 30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data." Sir Stanley Burton, *Report of the Interception Communications Commissioner, Annual Report for 2015*, Interception of Communications Commissioner's Office, at ¶¶ 7.23-7.24 (Sep. 8, 2016), available at: http://iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf.

10 월과 2016 년 10 월 사이에 메타데이터에 대한 48,208 건의 제공 요청이 있었는데, 이는 광범위한 카테고리의 통신자료이며 고객정보는 단지 적은 부분이었습니다.[55] 대략 인구가 6,600 만명이므로, 이는 1,375 명당 1 개의 메타데이터 요청이 있었음을 의미합니다. 미국의 인구는 약 314 백만 정도인데, 2012 년 이용자 개인정보 요청은 500,000 건에서 600,000 건 사이인 것으로 추정되며, 이는 대략적으로 600 명당 평균 1 건의 요청비율입니다.[56]

37. 사실상 한국의 1 인당 고객정보 요청 건수는, 그 다음으로 높은 수치를 보여주는 캐나다보다도 3.5 배가 많은 것입니다. 2011 년에 캐나다에서는 120 만건의 이용자 정보 제공요청(고객정보도 포함)이 있었습니다. 대략 3,400 만명의 인구가 있으므로, 위 수치는 캐나다인 28 명 당 1 건의 평균 요청이 있었음을 보여줍니다.[57] 더군다나 캐나다는 이용자 정보에 대하여 영장 없는 접근을 명시적으로 거절하고 있습니다.[58] 캐나다 형법에 따르면 정부의 이용자 정보 취득은 사법 명령에 의해 해당정보가 범죄의 증거를 제공할 수 있다고 "믿을 수 있는 합리적인 근거"를 확인하여야만

---

[55] *1er Rapport d'activité 2015/2016*, Commission Nationale de Contrôle des Techniques de Renseignment, at 65 (Nov., 2016) available at: https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf.

[56] Kyung Sin Park, Communications Surveillance in Korea, Korea University Law Review, Vol. 16-17, May 2015, at 61 - 62 (May, 2015), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2748318. These estimates are based on VERIZON, *Verizon's Transparency Report*, http://transparency.verizon.com/us-data, and calculated with reference to numbers that major U.S. telecommunications providers provided to Senator Edward J. Markey in 2012 and 2013. Ed Markey, *For Second Year in a Row, Markey Investigation Reveals More Than One Million Requests By Law Enforcement for Americans Mobile Phone Data*, ED MARKEY (Dec. 9, 2013), http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data; Ed Markey, *Markey: Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers*, ED MARKEY (July. 9, 2012), http://www.markey.senate.gov/news/press-releases/markey-law-enforcement-collecting-information-on-millions-of-americans-from-mobile-phone-carriers.

[57] *Response to Request for General Information from Canadian Wireless Telecommunications Association*, Office of the Privacy Commissioner of Canada, at 3 (Dec. 14, 2011), available at: *https://www.priv.gc.ca/media/1103/let_gowling_e.pdf*.

[58] *See R v. Spencer*, 2 S.C.R. 212 at 249 (June 13, 2014).

가능합니다.[59] 이러한 개인정보의 최소한의 요구는, 다른 덜 침해적인 신원확인수단이 있는 경우 통신사업자가 사회보장번호(캐나다의 주민등록번호와 동일함)를 수집하지 못하도록 하게 합니다.[60]

38. 대한민국의 국가기관이 이용자 정보를 요구하는 비율을 검토할 때, 이러한 요구가 영장 제시 없이 이루어지는 것은 표현의 자유에 대한 불필요하고 부적절한 침해 위험을 증가시킵니다.

VI. 결론

39. 이와 같이, 본인은 전기통신사업법 제 83 조 제 3 항 및 제 4 항이 대한민국의 인터넷 및 통신 사용자들의 표현의 자유에 대한 중대한 위험을 가져온다는 의견서를 제출합니다. 위 제 83 조 제 3 항 및 제 4 항은 전기통신사업자로 하여금 이용자 정보를 아무런 영장 제시가 없는 상태에서 국가기관에게 제공할 수 있도록 허용하고 있습니다. 이러한 제공 가능성 및 실제의 제공행위 자체는 규약 제 19 조 제 2 항에서 보호하고 있는 익명 표현 및 통신의 자유를 침해합니다. 국제법 및 실무의 분석결과, 국가기관의 이용자 정보 요구에 대한 사법 사전승인절차의 부재는 규약 제 19 조 제 3 항의 불필요하고 부적절한 제한을 구성합니다. 1 인당 이용자 정보 요구 수치가 가장 높은 대한민국의 현실에 의하여, 표현의 자유에 대한 위험은 더욱 악화될 것입니다.

40. 본인은 귀 재판소가 이러한 우려를 신중하게 판단하여 전기통신사업법 제 83 조 제 3 항 및 제 4 항의 헌법적 효력을 검토할 것을 촉구합니다.

---

[59] Canada Criminal Code § 487.018, RSC 1985, c C-46

[60] *See e.g.* Personal Identification Protection and Electronic Documents Act, Case Summary #2001-22, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/pipeda-2001-022/; Personal Identification Protection and Electronic Documents Act, Case Summary #2003-184, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-184/; Personal Identification Protection and Electronic Documents Act, Case Summary #2003-204, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-204/.

데이비드 케이

Respectfully Submitted,

DAVID KAYE

UN Special Rapporteur on the Right to Freedom of Opinion and Expression
Clinical Professor of Law and Director, International Justice Clinic, University of California Irvine School of Law
401 East Peltason Dr. Ste. 3800-C
Irvine, CA 92697-8000
(949) 824-2427
dkaye@law.uci.edu

산업 > **IT • 과학**

5년간 우리국민 7200만명 개인정보 털렸다

(서울=뉴스1) 이수호 기자 | 2017-09-27 09:50 송고

	개인정보 누출건수	누출 인원수	원인	
			해킹	확인불가
2012	17건	903,771명	14	-
2013	5건	187,209명	3	-
2014	66건	32,253,288명	32	31
2015	8건	6,184,521명	4	-
2016	21건	11,027,854명	17	1
합 계	**117건**	**72,109,271명**	**70**	**32**

*출처 : 방송통신위원회

최근 5년간 해킹으로 7200만명의 개인정보가 유출당한 것으로 집계됐다. 국민 1인당 1.4회 꼴로 털 린 셈이다.

국회 과학기술정보방송통신위원회 유승희 의원(더불어민주당)이 방송통신위원회로부터 제출받은 자료에 따르면 지난 5년간 방통위에 접수된 개인정보 유출 누적 인원수가 7200만명으로 집계됐다.

2012년 90만명에 불과했지만 2014년 3200만명으로 급증, 2015년에 하락세를 보였지만 다시 2016년에 1000만명의 개인정보가 유출됐다. 올해도 이미 여기어때와 빗썸, 남양유업 등에서 해킹 사고가 발생해 1000만명 이상의 개인정보가 유출된 상황이다.

유승희 의원은 "개인정보 유출을 시도하는 기술이 나날이 발전하고 있는 반면, 방송통신위원회가 그 속도를 따라가지 못하고 있는 것이 사실"이라며 "4차산업 시대는 기술의 발전과 개인정보 보호가 함께 이뤄져야 하기 때문에 개인정보보호를 위한 근본적인 대책 마련이 시급하다"고 강조했다.

ZDNet Korea news print

방송/통신

신분증 스캐너 허술..."위변조 못 걸러내"

통신 불법가입 차단 취지 무색…대책 시급

김태진 기자 입력 : 2016.11.23.17:06 수정 : 2016.11.24.14:38

이동통신 불법 가입자를 차단하기 위해 도입하기로 한 신분증 스캐너가 허점투성이인 것으로 드러났다.

방송통신위원회와 이동통신 3사는 오는 12월1일부터 모든 이동통신 대리점과 판매점 등 유통망에 신분증 스캐너를 전면 도입할 예정이다. 이에 따라 12월부터는 신분증 스캐너를 사용하지 않을 경우 이동통신 서비스 가입 자체를 할 수 없게 된다.

이 같은 조치는 이동통신 유통점에서 가입자 개인정보가 유출되는 것을 방지하는 한편 신분증을 복사해 명의도용을 하는 등 불법 가입자를 막겠다는 취지다.

하지만 본지가 이동통신 3사의 서비스를 모두 취급하는 판매점의 협조를 얻어 위변조 신분증으로 스캐너를 사용해 본 결과 정상적으로 가입할 수 있는 것으로 확인됐다. 신분증 스캐너가 홀로그램과 적외선, 빛 투과율 등으로 신분증의 위변조 여부를 판단하기 때문에 위조 신분증으론 가입이 불가능할 것이라는 방통위의 설명과는 전혀 다른 결과다.

신분증 스캐너

이번 실험에서 위변조 신분증은 스캐너가 정상적인 신분증으로 인식할 수 있도록 운전면허증을 컬러복사기로 복사한 뒤 운전면허증과 크기가 똑같은 이동통신사의 유심(USIM) 카드에 붙여서 만들었다. 여기에 적외선, 빛 투과율을 감안해 투명 스카치테이프와 비닐, 휴대폰 액정필름 등을 붙여 총 3종류의 위변조 신분증을 만들었다.

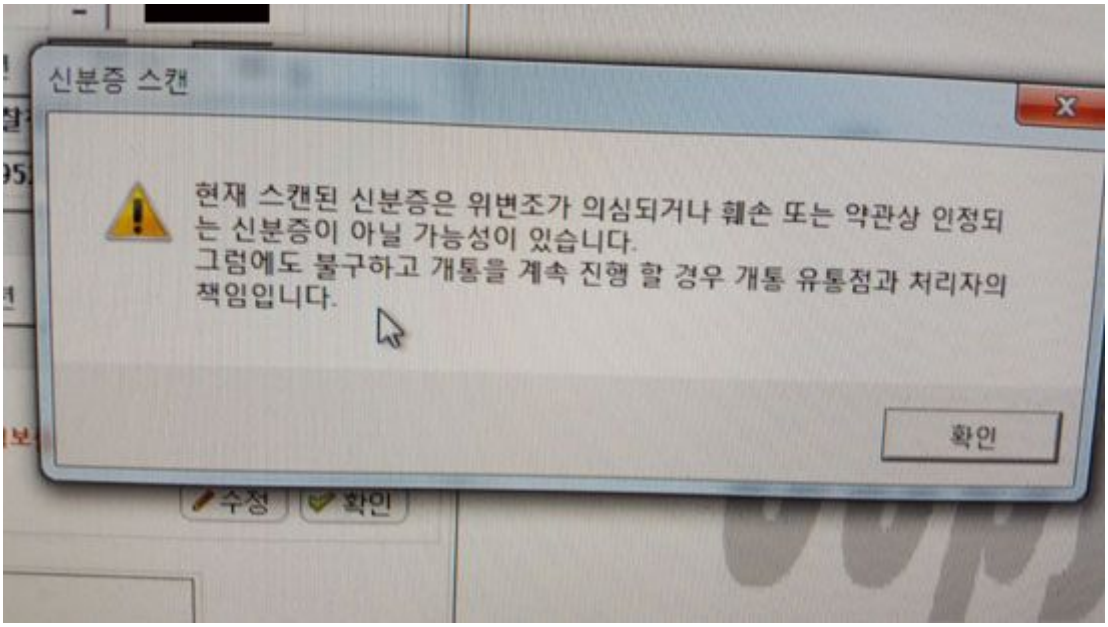
컬러복사기로 복사한 운전면허증

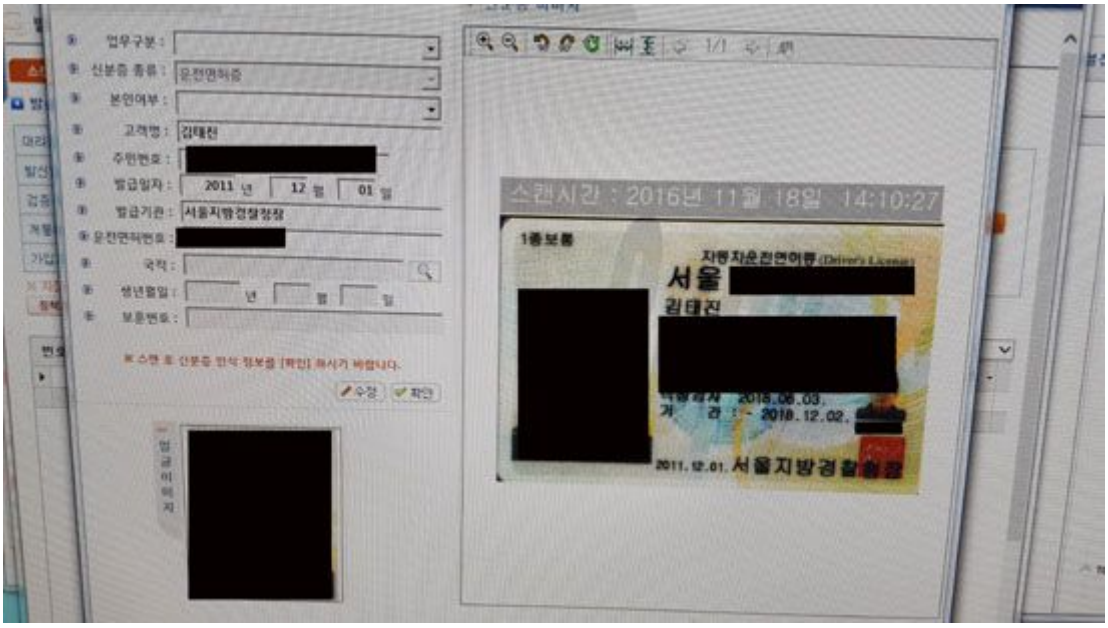
운전면허증과 크기가 똑같은 이동통신사의 유심 카드를 위변조 신분증을 만드는데 사용했다.

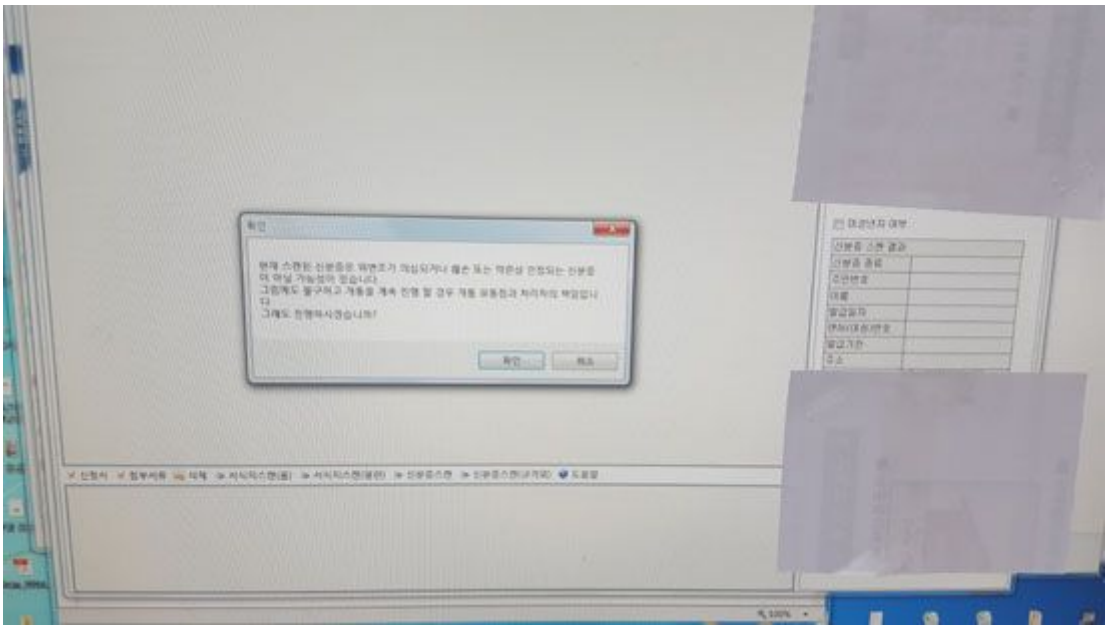
정상적인 운전면허증과 적외선, 빛 투과율을 감안해 투명 스카이테이프와 비닐, 휴대폰 액정필름 등을 붙여 만든 3종류의 위변조 신분증

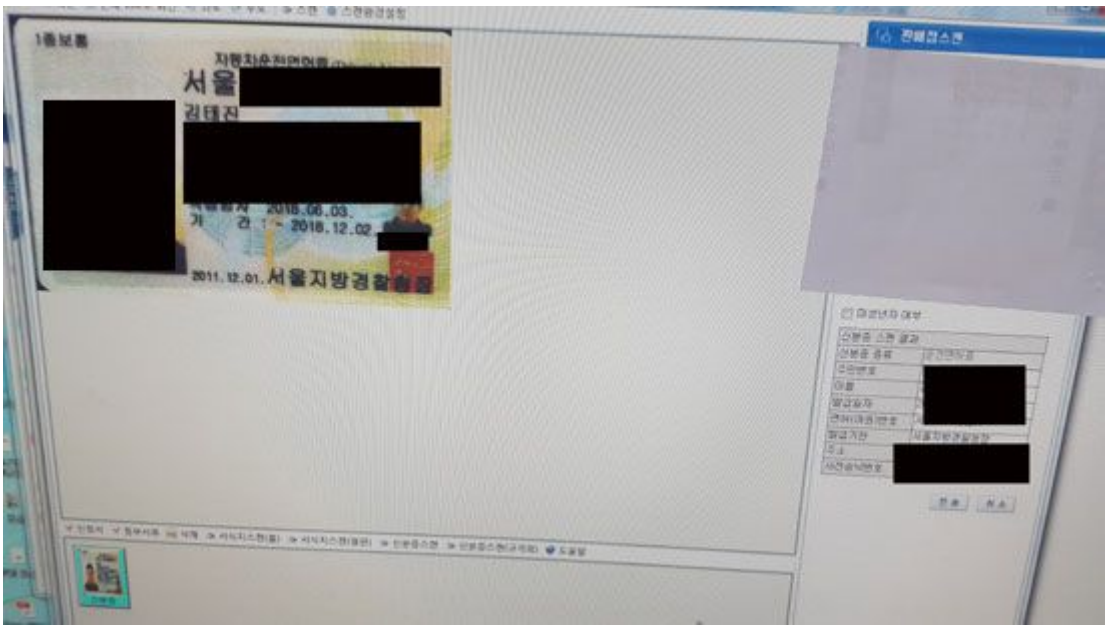
이렇게 만든 위변조 신분증으로 SK텔레콤, KT, LG유플러스의 이동전화 가입시스템과 연동된 신분증 스캐너에 통과시켜 가입절차를 진행했다.

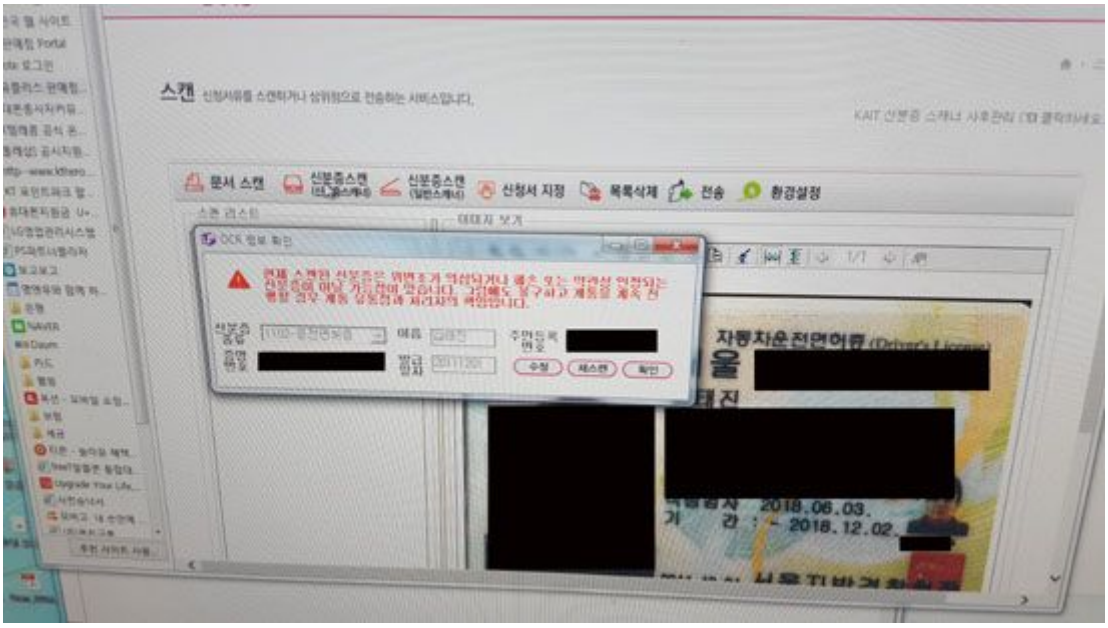
사용 결과 이동통신 3사 모두 '현재 스캔된 신분증은 위변조가 의심되거나 훼손 또는 약관상 인정되는 신분증이 아닐 가능성이 있다. 그럼에도 불구하고 개통을 계속 진행할 경우 개통 유통점과 처리자의 책임입니다"란 공통된 문구의 팝업창이 표시됐다.

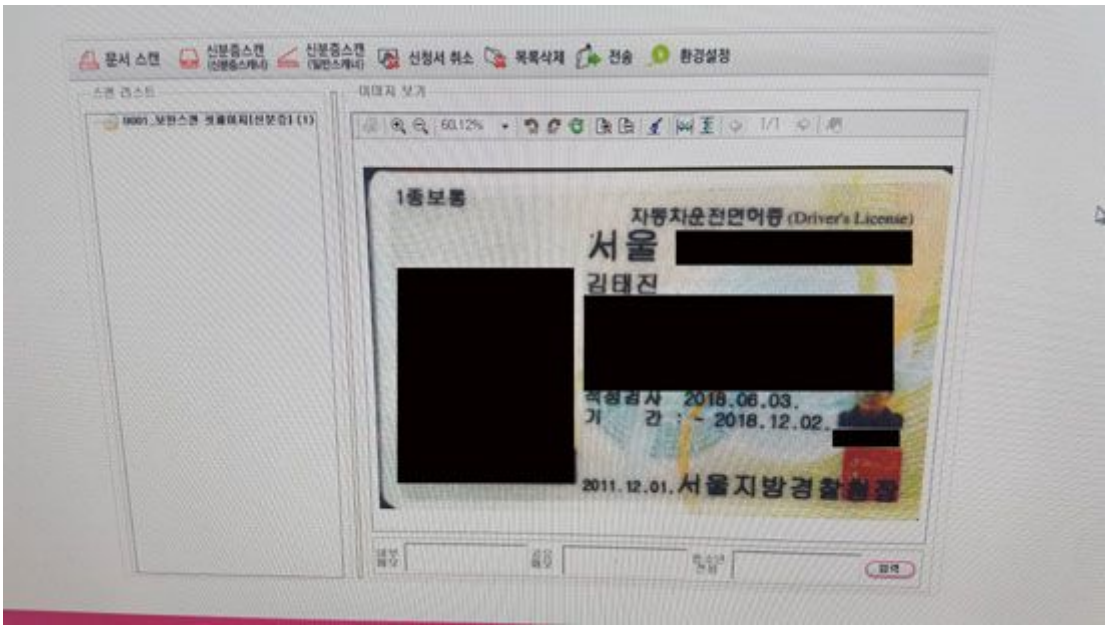



업무구분 :
신분증 종류 : 운전면허증
본인여부 :
고객명 : 김태진
주민번호 :
발급일자 : 2011 년 12 월 01 일
발급기관 : 서울지방경찰청장
운전면허번호 :
국적 :
생년월일 : 년 월 일
보훈번호 :
수정
확인
스캔시간 : 2016년 11월 18일 14:10:27
1종보통
서울
김태진
2011.12.01. 서울지방경찰청장


확인
확인
취소


1종보통
서울
김태진
2011.12.01. 서울지방경찰청장
전체스캔
확인
취소





스캐너에서 정상적인 인식이 가능하도록 신분증을 만들기는 했지만 홀로그램, 적외선, 빛 투과율 등 세 가지 적출값을 만족시키지 못해 이러한 '주의 메시지'가 나타난 것이다.

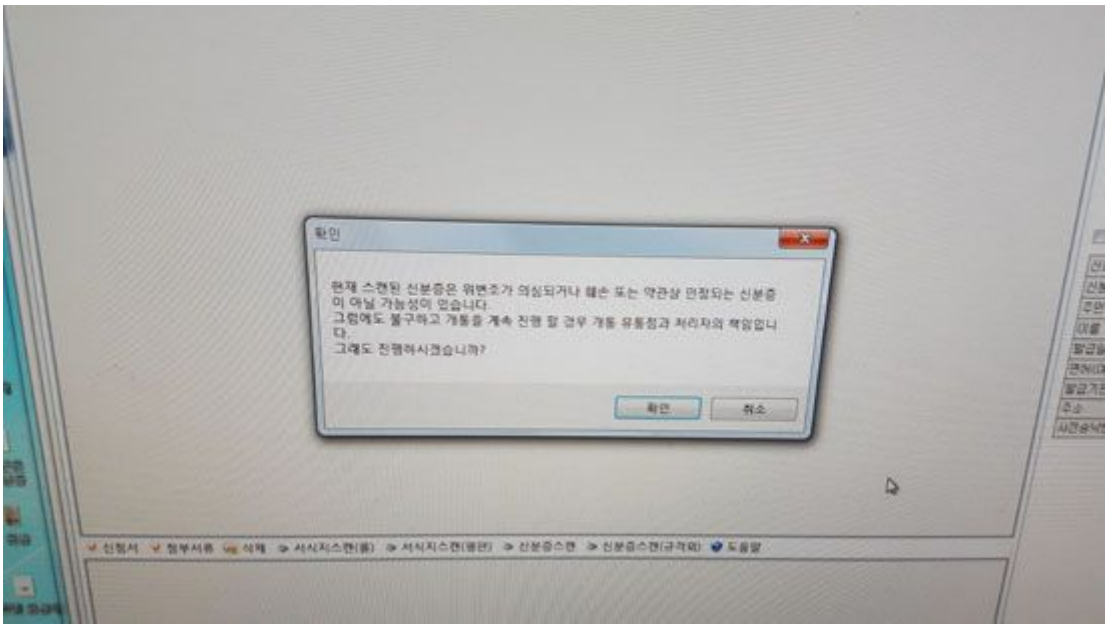
문제는 그 다음부터다. 주의 메시지에도 불구하고 '확인' 버튼 한 번 누르는 것만으로 다음 단계로 진행할 수 있었다. 이런 과정을 통해 정상적인 가입절차를 밟을 수 있었다. 이 같은 상황은 이동통신 3사 모두 똑 같았다.

특히, 위변조 신분증에서 불러온 가입자의 개인정보 역시 정상적인 신분증에서 불러온 데이터처럼 완벽하게 읽어 들였다.

위변조 신분증에서 읽어 들인 데이터로 개통을 진행해달라고 요청하자 판매점 직원은 "정상적으로 가입이 가능하다"며 "처음에 표시된 메시지 외에는 위변조 되지 않은 신분증을 사용했을 때와 다른 것이 없다"고 말했다.

아울러, 훼손된 신분증을 사용했을 때 어떠한 결과가 나오는지를 테스트하기 위해 정상적인 신분증에 작은 종이를 붙여 스캐너에 사용해봤다.

훼손된 신분증으로 인식시키기 위해 정상적인 운전면허증에 일부 정보를 읽어 들이지 못하도록 작은 종이를 붙였다.



이번에도 위변조 신분증을 사용했을 때처럼 '현재 스캔된 신분증은 위변조가 의심되거나 훼손 또는 약관상 인정되는 신분증이 아닐 가능성이 있다. 그럼에도 불구하고 개통을 계속 진행할 경우 개통 유통점과 처리자의 책임입니다'란 팝업창이 표시됐다.

결국, 위변조 신분증이나 훼손된 신분증 모두 스캐너에서는 같은 결과로 인식하고 동일한 메시지를 내보낸 것이다. 때문에 서비스에 가입하는 것도 가능했다.

■ "오히려 유통점 관리-감독 수단 아니냐" 불만도

따라서 현장에서 위변조 여부를 직접 확인하지 않는 이상 현재 시스템으로는 명의도용을 하는 등의 부정가입을 막는 것은 사실상 불가능하다는 결론이 나온다. 위변조로 의심되는 신분증을 사용했을 때 이동통신 가입을 원천 차단해 놓지 않았기 때문이다.

개인정보 유출 방지 또한 마찬가지다. 신분증 스캐너를 사용했을 때 가입자 정보를 캡처하지 못하도록 PC의 프린트 스크린 버튼을 막아놓긴 했지만 녹화 등의 방법으로 가입자 정보를 수집할 수 있는 만큼 디지털 시대에 이를 완벽히 차단하는 것도 사실상 불가능해 보인다.

오히려 팝업창으로 표시된 내용 중 '그럼에도 불구하고 개통을 계속 진행할 경우 개통 유통점과 처리자의 책임입니다'란 대목이 눈에 띈다.

유통업계 관계자는 "이런 메시지가 나올 때마다 이통사가 차감정책을 적용하겠다고 공지하면 유통점은 따를 수밖에 없는 구조"라며 "신분증 스캐너의 도입 취지와는 무관하게 이통사가 관리, 감독 수단으로 활용하려는 것 아니냐는 의심을 할 수밖에 없다"고 말했다.

실제, 지난 19일 오후 이동통신 3사는 스캐너 오류로 인한 '사용중단' 결정을 내리면서 유통점에 이로 인한 차감은 없다고 공지했다. 이날 스캐너 사용은 약 3시간 반 동안 중단됐다.

업계 한 관계자는 "수능 이후 부모들과 휴대폰을 구입하러 온 이용자들이 몰리면서 전산장애가 발생한 것으로 추정하고 있다"며 "스캐너가 주말에 장애를 일으켰을 때 복구가 불가능하고, 즉

각적인 대응이 불가능해 매출에 직접적 피해를 입을 수밖에 없다"고 말했다.

또 다른 업계의 한 관계자는 "단지 종이에 적던 가입신청서를 스캔하는 방식으로 바꿔놓았다고 정보유출이 안 된다고 생각하는 것은 디지털 시대에 순진한 발상"이라며 "정보유출이나 명의도용 등이 발생하지 않도록 업무 프로세스를 개선하거나 교육을 하고, 이러한 일이 발생했을 때 회복하지 못할 정도의 처벌을 하는 것이 오히려 개인정보 유출을 방지하는 길"이라고 말했다.

이어, "금융권에서 정부가 인증한 공인인증서를 사용했다고 금융사고 발생 시 이를 사실상 책임을 회피하는 면죄부처럼 활용해 왔던 것처럼 신분증 스캐너가 통신시장에서 그러한 용도로 활용될 가능성도 있다"고 꼬집었다.

tjk@zdnet.co.kr 김태진 기자

미래창조과학부 http://www.msip.go.kr	보 도 자 료	정책브리핑

보도일시	2017. 6. 5.(월) 배포시점부터 보도해 주시기 바랍니다.		
배포일시	2017. 6. 5.(월)	담당부서	통신서비스기반팀
담당과장	마재욱(02-2110-1909)	담 당 자	노진홍 사무관(1908)

'16년 하반기 통신자료 및 통신사실확인자료 제공 등 현황

□ 미래창조과학부(장관 최양희)는 기간통신사업자 50개, 별정통신사업자 55개, 부가통신사업자 35개 등 총 140개 전기통신사업자가 제출한 '16년 하반기 통신자료 및 통신사실확인자료 제공, 통신제한조치 협조 현황을 집계하여 발표하였다.

□ 미래창조과학부에 따르면, 전기통신사업법에 따라 '16년 하반기에 검찰, 경찰, 국정원 등에 제공된 통신자료 건수는 전년 동기 대비 전화번호 수 기준으로 883,177건(4,675,415→3,792,238건, △18.9%), 문서 수 기준으로 30,002건(564,847→534,845건, △5.3%) 각각 감소하였다.

○ '통신자료'는 통신서비스 가입자의 기본적인 인적사항(성명, 주민등록번호, 주소 등)으로서 통신기록이나 통화내용은 아니다.

○ 이러한 통신자료는 수사기관 등이 보이스피싱이나 납치 피해자 확인 등 신속한 범죄수사를 위해 전기통신사업법에 따라 공문으로 요청하여 전기통신사업자로부터 취득하게 된다.

□ 통신비밀보호법에 따라 '16년 하반기에 검찰, 경찰, 국정원 등에 제공된 통신사실확인자료 건수는 전년 동기 대비 전화번호 수 기준으로 858,582건(1,685,746→827,164건, △50.9%) 감소, 문서 수 기준으로 7,792건(150,062→157,854건, 5.2%) 증가하였다.

○ '통신사실확인자료'는 통화나 통신의 내용이 아닌 통화나 통신의 단순 내역(통화나 문자전송 일시, 착·발신 상대방의 가입자번호, 통화시간, 기지국 위치 등)이다.

○ 이러한 통신사실확인자료는 통신비밀보호법에서 정한 요건과 절차에 따라 수사기관 등이 법원의 허가를 받아 전기통신사업자로부터 취득한다.

□ 통신비밀보호법에 따라 '16년 하반기에 검찰, 경찰, 국정원 등의 통신제한조치 건수는 전년 동기* 대비 전화번호 수 기준으로 319건(2,155→2,474건, 14.8%), 문서 수 기준으로 11건(125→136건, 8.8%) 각각 증가하였다.

* 금번 통신제한조치 건수 집계과정에서 '14년 하반기~'16년 상반기 통신제한조치 건수에 오류가 있음이 발견되어 수정사항을 반영하였음(세부내역 붙임 참조)

○ 통신의 내용에 해당하는 음성통화내용, SNS메시지, 이메일 등에 대한 '통신제한조치'는 법원의 허가를 받아야 전기통신사업자로부터 취득할 수 있다.

○ 이러한 통신제한조치는 통신비밀보호법상 그 대상이 중범죄로 한정되어 있어 통신사실확인자료 제공보다 더욱 엄격한 제약하에서 이루어진다.

[붙 임] '16년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 1부. 끝.

이 자료에 대하여 더욱 자세한 내용을 원하시면
미래창조과학부 노진홍 사무관(☎ 02-2110-1908)에게 연락주시기 바랍니다.

[붙임]

'16년 하반기 통신자료 및 통신사실확인자료 제공 등 현황

Ⅰ. 통신자료 제공

수사기관이 수사 대상자의 인적사항을 통신사업자에게 요청하여 제공받는 제도 (전기통신사업법 제83조)

o 제공요청 사항
- 이용자 성명, 주민등록번호, 주소, 가입 및 해지일자, 전화번호, ID 등 가입자 정보

o 주요 절차
- 검·경찰, 정보수사기관은 검사, 4급이상 공무원, 총경 등이 결재한 제공요청서를 사업자에게 제시하여 이용자의 인적사항을 확인

□ 총괄 현황

o '16년 하반기 통신사업자들이 수사기관에 협조한 통신자료 제공건수는 전화번호 수 기준으로 3,792,238건, 문서 수 기준으로 534,845건
- 전년 동기 대비 전화번호 수 기준으로 883,177건(4,675,415→3,792,238건), 문서 수 기준으로 30,002건(564,847→534,845건) 각각 감소하였으며,
- 문서 1건당 전화번호 수는 평균 8.3개에서 7.1개로 1.2개 감소

□ 세부 내용별 현황

(1) 기관별

o 전년 동기 대비 전화번호 수 기준으로 검찰은 151,604건(1,287,204→1,135,600건), 경찰은 684,410건(3,235,624→2,551,214건), 국정원은 48,747건(63,231→14,484건) 각각 감소, 기타기관은 1,584건(89,356→90,940건) 증가

o 전년 동기 대비 문서 수 기준으로 검찰은 427건(100,790→100,363건), 경찰은 26,309건(432,844→406,535건), 국정원은 540건(2,022→1,482건), 기타기관은 2,726건(29,191→26,465건) 각각 감소

(단위 : 건)

구분		'15년		'16년	
		상반기	하반기	상반기	하반기
검 찰	전화번호수	1,449,034	**1,287,204**	1,072,869	**1,135,600**
	문서수	102,201	**100,790**	95,400	**100,363**
	문서1건당 전화번호수	14.2	**12.8**	11.2	**11.3**
경 찰	전화번호수	4,284,571	**3,235,624**	3,282,098	**2,551,214**
	문서수	421,468	**432,844**	450,221	**406,535**
	문서1건당 전화번호수	10.2	**7.5**	7.3	**6.3**
국정원	전화번호수	59,488	**63,231**	32,949	**14,484**
	문서수	2,130	**2,022**	1,527	**1,482**
	문서1건당 전화번호수	27.9	**31.3**	21.6	**9.8**
기타 기관*	전화번호수	108,571	**89,356**	92,350	**90,940**
	문서수	34,228	**29,191**	27,621	**26,465**
	문서1건당 전화번호수	3.2	**3.1**	3.3	**3.4**
합 계	**전화번호수**	5,901,664	**4,675,415**	4,480,266	**3,792,238**
	문서수	560,027	**564,847**	574,769	**534,845**
	문서1건당 전화번호수	10.5	**8.3**	7.8	**7.1**

* 기타기관 : 군 수사기관, 사법경찰권이 부여된 행정부처(관세청, 법무부, 고용노동부, 식품의약품안전처 등)

(2) 통신수단별

o 전년 동기 대비 유선전화는 7,233건(65,410→58,177건), 이동전화는 12,536건(451,152→438,616건), 인터넷 등은 10,333건(48,385→38,052건) 각각 감소

(단위 : 문서수)

구 분	'15년		'16년	
	상반기	하반기	상반기	하반기
유선전화	65,970	**65,410**	65,075	**58,177**
이동전화	441,799	**451,152**	463,444	**438,616**
인터넷 등	52,258	**48,385**	46,250	**38,052**
합 계	560,027	**564,847**	574,769	**534,845**

Ⅱ. 통신사실확인자료 제공

수사기관이 법원의 허가를 받아 수사 대상자의 통신사실확인자료를 통신사업자에게 요청하여 제공받는 제도 (통신비밀보호법 제13조 ~ 제13조의4)

o 제공요청 사항

- 상대방 전화번호, 통화 일시 및 시간 등 통화사실과 인터넷 로그기록·접속지 자료(IP Address) 및 발신기지국 위치추적자료

o 주요 절차

- 검찰, 경찰, 국정원 등 수사기관이 법원의 허가를 받아서 통신사업자에 자료제공을 요청

- 다만, 법원의 허가를 받기 어려운 긴급 상황시에는 요청서만으로 통신사실확인자료를 제공받을 수 있으나, 지체없이 법원의 허가를 받아야 함

□ 총괄 현황

o '16년 하반기 통신사업자들이 수사기관에 협조한 통신사실확인자료 제공 건수는 전화번호(또는 ID) 수 기준으로 827,164건, 문서 수 기준으로 157,854건

- 전년 동기 대비 전화번호(또는 ID) 수 기준으로 858,582건(1,685,746→827,164건) 감소, 문서 수 기준으로 7,792건(150,062→157,854건) 증가하였으며,

- 문서 1건당 전화번호 수는 평균 11.2개에서 5.2개로 6개 감소

□ 세부 내용별 현황

(1) 기관별

o 전년 동기 대비 전화번호 수 기준으로 검찰은 11,588건(83,570→95,158건) 증가, 경찰은 868,626건(1,597,667→729,041건), 국정원은 850건(1,263→413), 기타기관은 694건(3,246→2,552건) 각각 감소

o 전년 동기 대비 문서 수 기준으로 검찰은 3,858건(30,944→34,802건), 경찰은 4,262건(117,519→121,781건) 각각 증가, 국정원은 254건(457→203건), 기타기관은 74건(1,142→1,068건) 각각 감소

(단위 : 건)

구분		'15년		'16년	
		상반기	하반기	상반기	하반기
검 찰	전화번호수	84,826	**83,570**	68,637	**95,158**
	문서수	33,210	**30,944**	24,725	**34,802**
	문서1건당 전화번호수	2.6	**2.7**	2.8	**2.7**
경 찰	전화번호수	3,707,327	**1,597,667**	686,104	**729,041**
	문서수	115,771	**117,519**	119,258	**121,781**
	문서1건당 전화번호수	32.0	**13.6**	5.8	**6.0**
국정원	전화번호수	1,526	**1,263**	797	**413**
	문서수	524	**457**	221	**203**
	문서1건당 전화번호수	2.9	**2.8**	3.6	**2.0**
기타 기관*	전화번호수	5,520	**3,246**	2,952	**2,552**
	문서수	1,375	**1,142**	1,263	**1,068**
	문서1건당 전화번호수	4.0	**2.8**	2.3	**2.4**
합 계	**전화번호수**	3,799,199	**1,685,746**	758,490	**827,164**
	문서수	150,880	**150,062**	145,467	**157,854**
	문서1건당 전화번호수	25.2	**11.2**	5.2	**5.2**

* 기타기관 : 군 수사기관, 사법경찰권이 부여된 행정부처(관세청, 법무부, 고용노동부, 식품의약품안전처 등)

(2) 통신수단별

o 전년 동기 대비 유선전화는 2,710건(29,012→31,722건), 이동전화는 4,256건(102,985→107,241건), 인터넷 등은 826건(18,065→18,891건) 각각 증가

(단위 : 문서수)

구 분	'15년		'16년	
	상반기	하반기	상반기	하반기
유선전화	28,826	**29,012**	27,033	**31,722**
이동전화	104,019	**102,985**	106,572	**107,241**
인터넷 등	18,035	**18,065**	11,862	**18,891**
합 계	150,880	**150,062**	145,467	**157,854**

Ⅲ. 통신제한조치 협조

수사기관이 법원의 허가를 받아 통신사업자의 협조를 얻어 수사대상자의 통신 내용을 확인하는 제도 (통신비밀보호법 제5조 ~ 제9조의2)

o 확인 사항

- 통화 내용, 전자우편 등

o 주요 절차

- 일반 통신제한조치는 검찰, 경찰, 국정원 등 수사기관이 법원의 허가서를 받아 통신사업자에 협조를 요청하고,
- 긴급 통신제한조치는 검사 지휘서 또는 국정원장 승인서로 우선 협조 받되, 36시간 이내에 법원의 허가 등을 받아야 함

과년도('14년 하반기 ~ '16년 상반기) 발표현황 수정

o (대상) 미래부가 발표했던 '14년 하반기~'16년 상반기 통신제한조치 협조건수 일부

o (사유) '14년 하반기~'16년 상반기 동안 통신제한조치에 협조했던 일부 통신사에서 해당 기간 협조건수 산정 당시 오류가 있었음을 확인

※ 통신사들은 반기동안 협조한 통신제한조치 건수 산정 후 미래부에 보고 → 미래부 발표

< 수정내역 >

	'14년 하반기		'15년 상반기		'15년 하반기		'16년 상반기	
	수정전	수정후	수정전	수정후	수정전	수정후	수정전	수정후
전화번호수	1,851	2,683	2,832	4,147	1,314	2,155	2,407	4,209
문서수	192	195	203	209	120	125	165	175

o 미래부는 **통신제한조치**(감청) **협조 자료에 관한 실태점검 권한이 없어** 사전에 통계누락 및 착오 등을 **인지하기 어려웠던 상황**

※ 통신자료·통신사실확인자료에 대해서는 미래부에 실태점검 권한(통신비밀보호법 §13⑧)이 있으나, **통신제한조치**에 대해서는 **국회만이 현장검증 및 조사권한**을 **보유**(동법 §15②)

□ 총괄 현황

o '16년 하반기 통신사업자들이 수사기관에 협조한 통신제한조치 건수는 전화번호 수 기준으로 2,474건, 문서 수 기준으로 136건

- 전년 동기 대비 전화번호 수 기준으로 319건(2,155→2,474), 문서 수 기준으로 11건(125→136) 각각 증가하였으며,
- 문서 1건당 전화번호 수는 평균 17.2개에서 18.1개로 0.9개 증가

(단위 : 문서수)

구 분	'15년		'16년	
	상반기	하반기	상반기	하반기
일반 통신제한	209	**125**	175	**136**
긴급 통신제한	-	**-**	-	**-**
합 계	209	**125**	175	**136**

□ 세부 내용별 현황

(1) 기관별

o 전년 동기 대비 전화번호 수 기준으로 경찰은 13건(47→34건) 감소, 국정원은 332건(2,108→2,440건) 증가

o 전년 동기 대비 문서 수 기준으로 경찰은 4건(19→23건), 국정원은 7건(106→113건) 각각 증가

(단위 : 건)

구 분		'14년	'15년		'16년	
		하반기	상반기	하반기	상반기	하반기
검 찰	전화번호수	7	-	**-**	-	-
	문서수	4	-	**-**	-	-
	문서1건당 전화번호수	1.8	-	**-**	-	-
경 찰	전화번호수	108	41	**47**	19	**34**
	문서수	69	21	**19**	9	**23**
	문서1건당 전화번호수	1.6	2.0	**2.4**	2.1	**1.5**
국정원	전화번호수	2,568	4,106	**2,108**	4,190	**2,440**
	문서수	122	188	**106**	166	**113**
	문서1건당 전화번호수	21.0	21.8	**19.8**	25.2	**21.6**
*군 수사기관 등	전화번호수		-	**-**	-	-
	문서수		-	**-**	-	-
	문서1건당 전화번호수		-	**-**	-	-
합 계	**전화번호수**	2,683	4,147	**2,155**	4,209	**2,474**
	문서수	195	209	**125**	175	**136**
	문서1건당 전화번호수	13.8	19.8	**17.2**	24	**18.1**

* 군 수사기관 등 : 국군기무사령부, 국방부 등

(2) 통신수단별

o 전년 동기 대비 유선전화는 4건(52→48건) 감소, 인터넷 등은 15건(73→88건) 증가

(단위 : 문서수)

구 분	' 14년	' 15년		' 16년	
	하반기	상반기	하반기	상반기	하반기
유선전화	77	101	**52**	82	**48**
이동전화	-	-	**-**	-	**-**
*인터넷 등	118	108	**73**	93	**88**
합 계	195	209	**125**	175	**136**

* 인터넷 등 : 인터넷접속, 이메일 등

발간등록번호 31-9735044-001340-14

국회입법조사처 NATIONAL ASSEMBLY RESEARCH SERVICE

이슈와 논점

국회입법조사처

이슈와 논점 ▌제1135호 ▌2016년 3월 16일 ▌발행처 국회입법조사처 ▌발행인 임성호 ▌www.nars.go.kr

프라이버시 보호를 위한 통신자료 제공제도의 개선방향

심우민 *

1. 들어가며

최근 모바일 정보통신 기기 등의 활용이 급증하면서 통신 프라이버시 보호 요청이 강하게 제기되고 있다. 이에 따라 범죄수사 등 공익 목적을 위한 국가의 정보수집 방식에 대해서도 관심이 높아지고 있는 실정이다. 이와 관련한 현행 법상 제도들로는 통신제한조치(감청), 정보저장매체의 압수·수색, 통신사실확인자료 제공제도, 그리고 통신자료 제공제도 등이 있다.

이러한 제도들 대부분은 정보통신 환경의 변화로 인하여 개선 요청에 강하게 직면하고 있는 것이 사실이지만,[1] 이 중 '통신자료 제공제도'는 최근 수년간 주목할 만한 법원의 판결들[2]로 그 문제점이 부각되고 있다.

'통신자료'는 수사기관 등의 초동수사 단계에서 수사대상자 정보를 파악하기 위해 가장 빈번하게 활용되는 수단 중 하나이다. 그러나 이는 '인적사항 정보'를 의미하기 때문에 이용자 프라이버시 보호에 있어서도 상당한 중요성을 가진다.

이 글에서는 통신자료 제공제도를 둘러싼 쟁점들을 정리하고, 이에 대한 입법적 개선방향을 제시해 보고자 한다.

2. 통신자료 제공제도의 법령상 체계

(1) 통신자료의 의미

통신자료 제공제도는 「전기통신사업법」 제83조 제3항 이하에 규정되어 있다. 즉 법원, 검사 또는 수사관서의 장, 정보수사기관의 장이 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 통신자료 제출을 요청하면 전기통신사업자는 이에 따를 수 있다.

통신자료에는 이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입 및 해지일이 포함된다. 이는 이용자 '인적사항'으로 현행 개인정보 보호법제에서 규정하고 있는 개인정보(개인식별정보)에 해당한다.

(2) 규정의 성격

통신자료 제공제도를 규정하고 있는 「전기통신사업법」 제83조 제3항은 수사기관 등이 통신자료를 요청하는 경우에 전기통신사업자는 "그 요청에 따를 수 있다"고 규정하고 있는데, 이

1) 예를 들어, 최근 대법원 2015.7.16. 2011모1839 결정은 정보저장매체의 압수·수색을 통한 정보취득의 범위의 포괄성을 제한하였다.

2) 서울고등법원 2012.10.18. 2011나19012 판결은 수사기관 등의 제공요청에 대한 사업자들의 기계적 수용관행에 제동을 걸었으나, 최근 대법원 2016.3.10. 2012다105482 판결은 이를 파기환송하여 논란이 일고 있다. 또한 서울고등법원 2015.1.19. 2014나2020811 판결은 이동통신사업자의 통신자료 제공현황 공개의무를 인정하였다.

* 사회문화조사실 과학방송통신팀 입법조사관, 법학박사, 788-4714, legislation21@nars.go.kr

규정이 과연 강행적 성격을 가지는지 여부가 문제시 된다.

이에 대해 헌법재판소는 수사기관 등의 이용자에 대한 통신자료 제공요청에 응할 것인지 여부는 전기통신사업자의 재량(법적판단 및 형량)에 맡겨져 있다고 판단하였다.[3)]

(3) 요청 및 제공의 통제수단

「통신비밀보호법」상 통신제한조치 및 통신사실확인자료 제공요청 등과는 달리, 「전기통신사업법」상 통신자료 제공요청에 있어서는 법원의 허가 및 이용자에 대한 사후 통지와 같은 법적요건이 존재하지 않는다. 다만 동법은 수사기관 등이 통신자료 제공을 요청하기 위해서는 서면(자료제공요청서)[4)]에 의할 것만을 규정하고 있다(제83조 제4항).

이와 대조적으로, 전기통신사업자들에게는 제공사실을 기재한 대장 및 자료제공요청서의 비치의무, 제공현황 보고의무, 관련 행정기관장에게 대장의 내용을 알릴 의무, 자체적인 통신비밀 전담기구의 설치·운용 의무 등을 「전기통신사업법」 제83조 제5항 이하에서 규정하고 있다.[5)]

3. 개선의 필요성

(1) 제도적 연혁

현재 시점에서 통신자료 제공제도 개선의 필요성을 명확히 하기 위해서는, 이 제도의 연혁에 대해 먼저 검토할 필요가 있다.

통신자료 제공제도는 1983년 12월 30일 제정된 「공중전기통신사업법」 규정에서부터 유래한다. 당시 동법 제82조 제2항은 "공사·전신업무취급국·전화업무취급국 또는 제5조의 규정에 의하여 공중통신사업의 일부를 수탁취급하는 자는 수사상 필요에 의하여 관계기관으로부터 공중통신업무에 관한 서류의 열람·제출의 서면요구가 있는 때에는 이에 응할 수 있다"고 규정하고 있었다.

이후 통신 환경의 변화를 반영하여 1991년 8월 10일 위 법률의 제명을 「전기통신사업법」으로 변경하였으며, 2000년 1월 28일 동법 개정에서는 통신자료 제공 요청 주체(수사기관 등) 및 절차 등에 관한 규정이 추가되었다. 이후 2010년 3월 20일 「전기통신사업법」이 전면 개정되면서 통신자료 제공제도가 현재의 조문 위치인 동법 제83조 제3항 이하에 규정되기에 이르렀다.

이상의 연혁으로 알 수 있듯이, 현행 통신자료 제공제도는 사실상 유선전화 시절의 체계를 상당부분 유지하고 있다. 따라서 이 제도의 개선 필요성이 강하게 제기되고 있으며, 실제로 제19대 국회에서도 이에 관한 개정 법률안들이 다수 발의되었다.

[표 1] 통신자료 제공 관련 개정법률안

발의일	대상법률	대표 발의	요청 요건	비고
15.11.17	전기통신사업법	서상기	완화	
15.11.16.	전기통신사업법	유승희	강화	
15.8.21.	전기통신사업법	전해철	강화	통비법 이관
15.8.4.	전기통신사업법	황인자	완화	
15.6.12.	통신비밀보호법	전해철	강화	
15.5.14.	전기통신사업법	김한길	강화	
15.2.27.	전기통신사업법	김광진	강화	폐지
14.12.29.	전기통신사업법	윤재옥	완화	자살예방
14.12.9.	전기통신사업법	정청래	강화	
14.12.8.	전기통신사업법	임수경	강화	
14.1.16	통신비밀보호법	송호창	강화	가입자정보
13.5.15.	전기통신사업법	변재일	강화	
13.1.15.	전기통신사업법	이만우	강화	
12.11.2.	통신비밀보호법	서영교	강화	통비법 이관
12.10.30.	전기통신사업법	강창일	강화	

* 출처: 국회의안정보시스템

3) 헌재 2012.8.23. 2010헌마439. 이러한 헌법재판소 결정의 맥락에서 서울고등법원 2012.10.18. 2011나19012 판결도 사업자의 손해배상책임을 인정한 것이었다.

4) 미래창조과학부, 「통신자료 요청 및 제공 업무 처리 지침」, 2014. 12. 30, [별표] 참조.

5) 이러한 전기통신사업자의 제반 의무는 「통신비밀보호법」상 통신제한조치 및 통신사실확인자료 관련 조항들에서도 유사하게 규정되어 있다.

(2) 통신환경의 급격한 변화

현대적인 모바일 통신환경에서는 사실상 기기와 이용자가 일대일로 대응한다고 볼 수 있어, 과거 통신자료 제공에 비하여 더욱 더 기본권(개인정보자기결정권 및 표현의 자유) 제약의 가능성이 커졌다고 평가할 수 있다.

특히 우리나라의 경우에는 주민등록번호, 아이핀 등과 같은 개인 식별정보의 범용적 활용이 입법적으로 제도화 되어 있어,[6] 단순한 이용자 인적사항에 관한 정보라고 할지라도 범죄수사 등 공익적 필요성을 넘어서서 당해 이용자의 사생활의 상당부분을 추적하는 것이 가능하다. 물론 2012년 헌법재판소의 인터넷 게시판 본인확인제에 대한 위헌결정[7]이 있었지만, 실제 컨텐츠 접속 및 이용의 관문(gateway) 역할을 하는 휴대전화 및 통신망 가입시 본인확인이 의무화되어 있어[8] 상황이 크게 변화되었다고 보기 어렵다.

이상과 같은 우리나라의 특수한 통신환경에 비추어 본다면, 범죄수사 등 공익적 목적의 실현은 물론이고, 이용자들의 기본권 보장의 문제도 더욱 면밀하게 검토할 필요가 있다. 즉 공익과 사익에 대한 엄밀한 입법적 형량이 요구된다.

(3) 수사 관행 및 편의성 문제

이제까지 일반적으로 통신자료 제공제도는 초동수사 단계에서 수사대상자 등의 인적사항을 확인하기 위한 편의적 목적으로 빈번하게 활용되어 왔다. 그러나 통신 프라이버시에 대한 사회적 관심이 높아지면서 이러한 관행의 개선이 요구되고 있다.

특히 통신자료 제공행위에 대한 법원의 2012년 손해배상 판결[9] 이후, 포털 사업자들은 제공여부에 관한 법적판단의 어려움을 이유로 수사기관 등의 제공요청에 응하지 않아 왔다.

그러나 이러한 상황은 주요 포털 사업자들에 한정하는 것으로, 여타 전반적인 통신자료 제공 건수는 오히려 지속적인 증가추세에 있는 것으로 확인된다.

[표 2] 통신자료 제공건수(단위: 문서수)

11년	12년	13년	14년	15년(상)
651,185	820,800	944,927	1,001,013	560,027

* 출처: 방송통신위원회 및 미래창조과학부 보도자료(2011년~2015년 상반기).

또한 주요 포털사들이 통신자료 제공요청에 응하지 않고 있는 상황으로 인하여, 수사기관 등이 정보저장매체(서버 등)의 압수·수색 등과 같이 통신자료 제공제도에 비하여 기본권 제한 가능성이 더욱 높은 수사방식을 취하게 되는 것은 아닌지, 즉 수사편의에 치중한 불필요한 정보수집의 우려가 제기된다.

실제 관련 통계들을 확인해 보면 이러한 문제인식의 타당성을 전적으로 부인하기 힘든 측면이 있다. 즉 포털 사업자들의 통신자료 제공이 중단된 2012년 이후 정보저장매체의 압수·수색 건수는 전반적으로 비교적 가파른 증가추세를 보여주고 있다.

---

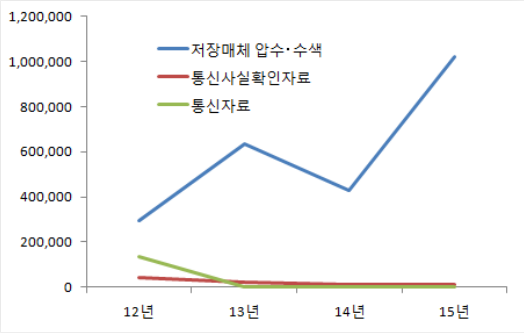
6) 심우민, 「인터넷상 아이핀 등 범용 개인 식별정보 활용의 문제점과 과제」, 『이슈와 논점』 제976호, 2015.4.16.

7) 헌재 2012.8.23, 2010헌마47, 252(병합).

8) 이는 소위 '휴대전화 실명제'라고도 불린다. 특히 현행법은 대포폰 등 부정이용 방지라는 목적으로 「전기통신사업법」 제32조의4 및 제32조의5 등의 규정을 2014년 10월 신설하여, 전기통신사업자들로 하여금 전기통신역무제공 계약의 체결시 가입자(이용자) 본인확인을 하도록 강제하고 있다.

9) 서울고등법원 2012.10.18. 2011나19012. 그러나 최근 대법원은 사업자들의 손해배상 책임을 부인하는 취지로 이 판결을 파기환송하였다. 즉 대법원은 수사기관의 권한남용이 있는 경우 이에 대한 통제는 국가나 해당 수사기관에 대하여 직접 이루어져야 한다고 하면서, 사업자에게 법적판단 의무를 부과하는 것은 수사기관 등의 책임을 사인(私人)에게 전가시키는 것이라고 판시하였다. 대법원 2016.3.10. 2012다105482.

[그림 1] 주요 포털의 수사협조 건수



* 출처: 카카오, 「투명성 보고서」, 2016.1; 네이버, 「투명성 보고서」, 2016.1 참조 및 정리.

결과적으로 통신자료 제공제도의 운용방식은 궁극적으로 통신 프라이버시와 연계된 다른 제도들과 상호 연관성을 가진다. 따라서 제도개선 논의에서 단편적인 수사상 편의성에만 치중하게 되면 실질적인 이용자 프라이버시 보호는 어려워질 수 있다.

4. 입법정책적 개선방향

(1) 통신 패러다임의 변화 고려

현행 통신자료 제공제도는 당초 제도 도입당시의 유선전화 중심의 체계를 사실상 그대로 유지하고 있다. 그러나 향후 프라이버시 침해 강도가 높은 이용자 밀착형 통신기술의 발전이 지속될 것으로 보여, 이러한 상황적 변화에 대한 고려가 필수적으로 요구된다.

물론 이러한 고려는 비단 통신자료 제공제도에 국한된 것은 아니다. 실질적 프라이버시 보장을 위해서는 「통신비밀보호법」 등에 규정되어 있는 유관 제도들(통신제한조치, 정보저장매체의 압수·수색, 통신사실확인자료 제공제도 등)과의 연계성 속에서 개선 논의가 이루어질 필요가 있다.

(2) 사업자 법적판단의 여지 경감

통신 프라이버시 보호를 위한 전기통신사업자들의 자체적인 노력은 상당히 중요하다고 할 수 있다. 그러나 '프라이버시 관련 정보 제공여부에 대한 법적판단(형량)'을 사업자측에 상당 부분 전가시키는 '입법대안'의 구성은 지양[10] 할 필요가 있다.[11]

사업자가 법적판단을 하게 되는 경우, 그로 인해 발생할 수 있는 소송위험 또한 사업자 스스로 부담할 수밖에 없다. 이는 정보통신서비스 제공자들의 국내외적 경쟁력을 제약하는 결과를 초래할 수 있다.

(3) 실질적 사전·사후 통제방안 모색

수사목적 정보수집의 불가피성을 인정한다고 할지라도, 이로 인해 개인정보자기결정권 및 표현의 자유에 대한 과도한 제한이 이루어질 수 있어 유의할 필요가 있다.

따라서 통신자료 제공요청에 대한 실효적인 사전 및 사후 통제방안이 필요하며, 현재는 영장주의 및 사후통지 대안이 논의 중에 있다. 이와 관련해서는 초동 및 임의수사 단계에서 통신자료가 활용된다는 점을 고려하여 추가적인 조정 및 대안마련이 필요할 것으로 보인다.

5. 나가며

지난 수년간 답보상태에 있는 통신자료 제공제도 개선을 위해서는, 단순히 수사상 편의성뿐만 아니라 변화된 통신환경 속에서의 실질적인 이용자 프라이버시 보호방안까지 균형성 있게 고려할 필요가 있겠다.

❑ 「이슈와 논점」은 국회의원의 입법활동을 지원하기 위해 최신 국내외 동향 및 현안에 대해 수시로 발간하는 정보 소식지입니다.

10) 이는 입법의 방향성을 의미한다. 이와 관련한 사법판결에 있어서는 헌재 2012.8.23. 2010헌마439 결정과 대법원 2016.3.10. 2012다105482 판결 간의 논리적 상충을 어떻게 조화시킬 수 있는지 여부가 향후 관건이라고 할 수 있다.

11) 그렇다고 임의적인 현행 규정을 단순하게 '수사기관 등의 통신자료 제공요청에 사업자가 반드시 따라야 한다'고 개정하게 되면 이용자 프라이버시를 과도하게 침해할 가능성이 있다.