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