

PRIVACY INTERNATIONAL

프라이버시 인터내셔널

대한민국 헌법재판소
사건번호 2016 헌마 388

프라이버시 인터내셔널의 제3자 의견서 제출

프라이버시 인터내셔널
62 브리튼 스트리트
런던 EC1M 5UY, 영국
Tel: +44 20 3422 4321
www.privacyinternational.org

2017. 4. 10.

I. 서문

1. 프라이버시 인터내셔널은 대한민국 헌법재판소 (이하 “한국”)에 정보통신사업법 제 83와 84 조 관련 사생활과 표현의 자유에 관한 헌법소원청구소송에 제 3자 의견서를 제출합니다. 프라이버시 인터내셔널은 특별히 이 두 권리를 행사하는데 있어서 익명성의 중요성과 정보통신사업법이 수백만 한국인의 익명 표현의 자유를 침해하고 있음을 강조하고자 합니다.

II. 프라이버시 인터내셔널의 활동분야

2. 프라이버시 인터내셔널은 영국 런던에 위치한 비영리, 비정부 단체로 전세계 사생활의 자유를 수호하기 위해 일하고 있습니다. 1990 년에 설립된 프라이버시 인터내셔널은 정부 및 기업의 감시와 감시를 위해 사용되는 기술에 관한 연구와 조사를 실시하고 있습니다. 우리기관은 미국, 영국, 유럽 등 전세계 법정에 사생활의 자유와 관련된 사건에 법정조언자 의견서를 제출하여 소송에 참여하고 있습니다. 전세계 사생활의 자유 존중을 위해서 프라이버시 인터내셔널은 이 권리를 보호하는 국내, 지역, 국제법 옹호 활동을 하고 있습니다. 또한 사생활의 자유 위협요소를 식별하고 보호하기 위해 개발국가의 관련 기관 역량 강화에 힘쓰고 있습니다.

III. 논의

A. 익명성과 익명 표현의 중요성

3. 익명성과 익명 표현의 자유는 인류 역사에 있어서 중요한 기반이 되어 왔습니다.¹ 익명성은 개인이 사생활과 표현의 자유를 침해하는 불법적 행위를 경감하거나 피하는 중요한 도구 중 하나이며, 국가기관의 통제로부터 자유롭게 정보를 주고받는 권리를 향유하게 하는 수단이 되어 왔습니다. 이와 같이 익명성은 전통적으로 사생활의 자유와 개인정보보호와 연결되어 왔으며², 표현의 자유를 행사하는데 중요한 안전망의 역할을 해왔습니다.³

¹ 법적 권리로서의 익명성: 어디에 적용되고 왜 중요한가, 16 N.C. J.L. & Tech. 311 호, 2015, 317-331. 참고 (표현의 자유와 관련하여 익명성의 역사적 중요성을 논함).

² Rotaru v. Romania 사건, 신청번호 28341/95, 2000.05.04, 42 문단, 유럽인권재판소는 유럽인권협약의 8 조가 보호하는 개인의 사생활은 익명성을 내재한다고 판시함.

³ 아티클 19 조, 온라인 익명권, 2015.06.18, p. 1.

https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_fi nal-web.pdf.

4. “간단히 말하자면, 익명성은 식별되지 않는다는 ‘사실’ 이고, 이것은 많은 사람들이 군중 속을 걷는다거나 낯선 사람들과 줄을 서는 등 일상에서 겪는 평범한 경험입니다.”⁴ 따라서 “어떤 활동은 공개적이지만 동시에 익명으로 가능한 것입니다.”⁵ 개인이 신분을 비밀로 유지하며 동시에 공개적으로 활동할 수 있다는 것이 바로 익명성의 유익을 말해줍니다. 이것은 개인이 자유롭게 정부나 권력기관에 관한 비판하고 부정을 폭로하는 일을 가능하게 합니다.⁶
5. 이러한 맥락에서 유럽인권재판소는 익명성의 중요성을 강조하고 익명성은 “보복이나 원치 않는 관심을 피할 수 있게 하며” 따라서 “자유로운 생각과 정보의 흐름의 증진을 가능하게 하며 특히 이것은 인터넷상에서 중요한 점입니다.” 이라고 적시했습니다.⁷ 미국 대법원 역시 익명 표현을 “이이 제기와 권리옹호 활동의 명예로운 전통” 이라고 표현하며 “다수의 횡포를 막는 방패” 인 익명 표현의 자유의 역사적 중요성을 역설하였습니다.

익명으로 작성된 팜플렛, 전단지, 브로셔와 책 등은 인류발전에 있어서 중요한 역할을 해왔습니다. 역사적으로 탄압받았던 단체나 집단은 억압적인 관행 또는 법률에 항거해 오직 익명으로만 비판을 제기할 수 있었습니다. 영국 식민지에는 정부에 비판적 논조 언론의 허가에 관한 법률이 시행되었었는데, 이 법률이 시행되면 출판사, 작가, 배급사들의 이름을 공개하면 비판적 문헌들의 발행이 줄어들 것이라는 이유 때문이었습니다. 이러한 예전 영국 불온문서에 대한 명예훼손 사건들은 통치자에게 비판적인 서적을 발간한 책임자를 찾아내기 위해 정부가 들인 노력을 보여줍니다.⁹

6. 역사전반에 걸쳐 익명성은 개인을 국가, 같은 국민 또는 세계 어디에나 있을 수 있는 잠재적 억압자로부터 보호막이 되어 왔습니다.¹⁰ 이 개인들은 정부기관이나

⁴ 상동, p. 10.

⁵ 상동.

⁶ 프라이버시 인터내셔널, 온라인에서의 안전 공간 확보, 2015.06. p.8.

https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf.

⁷ Delfi AS v. Estonia, 신청번호 64569/09, 2015.06.16, 147 문단.

⁸ McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995), p. 357.

⁹ Talley v. California, 362 U.S. 60 (1960), pp. 64-65.

¹⁰ 프라이버시 인터내셔널, 유엔 표현의 자유 특별 조사 위원에 제출된 문서-디지털 커뮤니케이션에서의 익명성과 암호화, 2015.02, p.2 (<http://www.ohchr.org/Documents/>

사기업에 의해 자행된 권력남용을 폭로하려는 내부고발자들이었습니다. 이 사람들은 경제적 취약층과 정부간의 소통을 확대하려는 반체제 인사들이었으며, 공공기관과 민간기관의 투명성, 검증성 확보를 위해 필요한 정보를 제공하던 언론인들이었고, 익명성이 주는 보호막이 없이는 자신들이 겪는 난관과 시련을 논의하기 어려웠던 보통 사람들이었습니다.¹¹ 이 모든 사람들에게 익명성은 “불필요하고 부당한 검증 없이 생활을 영위할 수 있도록 개인의 자유를 보장해 주었습니다.”¹² 그리고 “익명성은 수많은 인터넷 사용자들이 중요시하는 가치이며, 이것이 견고한 온라인 논의의 장을 형성하는데 큰 기여를 했다는 점은 놀랍지 않습니다.”¹³

7. 인터넷의 출현과 현대기술이 혁신적으로 변화시킨 소통방법 때문에 익명성과 익명 표현의 자유는 현대사회에서 위협받고 있습니다.¹⁴ 전세계의 사람들, 특히 대한민국 국민들은 대부분의 시간을 온라인에서 보내고 있습니다.¹⁵ 이들은 아이디어를 전달하고, 연구를 하고, 사랑하는 사람과 소통하며 정치적, 개인적 견해를 표현하는데 인터넷을 사용합니다. 또한 기록을 남기고, 여행을 계획하고 금융거래를 하는 등의 일상생활에도 인터넷이 사용되고 있습니다. 이 활동 중 많은 부분은 개인, 직장생활에 자연스럽게 스며든 휴대 전자 기기로 이루어 집니다. 이 기기들은 줄로 고정된 전화기, 서류정리함, 사진첩과 주소록을 대체하였고 이들의 기능을 통합하였습니다.
8. 인터넷은 사람들이 소통하는 방법을 급격하게 변화시켰을 뿐만 아니라 소통의 빈도와, “커뮤니케이션 데이터” 또는 “메타데이터” 로 알려진 개인 정보 커뮤니케이션의 양적 증가에도 기여했습니다. 커뮤니케이션 데이터는 송신자, 수신자, 정보가 보내진 장소와 날짜, 정보를 보낸 기기의 종류를 포함하는

Issues/Opinion/Communications/PrivacyInternational.pdf.) 참고. 전자 프로티어 재단, 익명성 ,(<https://www.eff.org/issues/anonymity>.) 참고.

¹¹ 가브리엘라 콜만, 온라인 익명성은 모두에게 유익하다, 뉴욕타임즈, 2014.08.20. ,(<http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls/anonymity-online-serves-us-all>.) , “신문의 기명 논평 페이지 역시 동일하게 주요하지만 익명 발언은 보다 더 보편적인 형태이다. 예컨대 민감한 주제를 논하고자 하는 환자나 환자의 양육자는 익명 포럼이 필요하며..(중략).. 혐오범죄의 피해자 역시 이야기를 털어 놓는데 있어 익명성을 사용한다. 익명성은 비슷한 경험을 공유하는 피해자들에게 위안을 제공하고 가해자에게 대항하여 말할 용기를 준다.”

¹² 아티클 19 조, 온라인 익명권, 노트 3, p. 10.

¹³ 프라이버시 인터네셔널, 온라인에서의 안전 공간 확보, 노트 6, p. 8.

¹⁴ 유엔 인권 이사회(2014), 디지털 시대 사생활 권리, 유엔인권최고대표사무소의 보고서, 2014.06.30, A/HRC/27/37, 1 문단 (현대 디지털 커뮤니케이션 기술의 편재성에 대해 논함).

¹⁵ 프론티어 월드, 한국 : 지구상 가장 인터넷에 연결이 많이 된 나라, PBS, 2009.04.14,(http://www.pbs.org/frontlineworld/stories/south_korea802/).

정보입니다. 디지털화된 세계에서는 커뮤니케이션 데이터가 개인의 의료기록이나 종교적 관점, 정치적 성향이 드러날 수 있는 인터넷 방문기록을 포함하는 등 더 많은 내용을 기록할 수 있습니다. 구입한 물건, 방문한 뉴스 사이트, 가입한 게시판, 읽은 책과 본 영화, 게임 등 각각의 커뮤니케이션 데이터는 한 개인에 대한 통찰을 가능하게 합니다.

9. 커뮤니케이션 데이터를 모으면 개인의 사적 관계, 관심사, 위치정보나 활동내역 등이 밝혀지는 침해적이고 포괄적인 관점을 가능하게 합니다. 무엇보다도 가입자 정보는 커뮤니케이션 데이터와 결합되어 한 개인이 어떤 사람인지 정확히 식별하는 것을 더욱 쉽게 만듭니다. 예를 들어 가입자정보를 획득하게 되면 개인을 특정 대화나 장소, 시간과 연결할 수 있어 정부기관은 이미 수집된 다른 커뮤니케이션 데이터와 개인의 이름, 전화번호의 연관성만 찾으면 됩니다. 따라서 익명의 “x” 라는 구체적인 묘사가 정부에게는 식별된 특정개인의 구체적인 묘사로 알려지게 되는 것입니다.
10. 익명성은 사생활과 자유로운 생각의 교환에 너무나 중요하기 때문에 법정과 인권전문가들은 적법성, 필요성, 과잉금지의 원칙 등 관련 인권 기준에 따라 익명성을 침해하는 요소에 관한 평가를 시작했고 침해적 요소가 있을 경우 사람들의 보호를 위해 더 엄격한 절차적 보호조치를 요구했습니다.¹⁶

B. 익명성을 사생활과 표현의 자유권의 권리로 인정하려는 국제적 법률 전문가들의 움직임

11. 국제법 전문가들은 익명성 침해요인들을 관련 인권 기준으로 분석해야 한다고 주장해 왔습니다.
12. 전·현직 의사·표현의 자유 증진과 보호를 위한 유엔 특별보고관은 꾸준히 표현의 자유의 일부분으로써의 익명성을 지지해 왔습니다. 프랭크 라튀 특별보고관은 2011년 이미 사생활의 자유와 온라인상 표현의 자유 사이 상호관계를 확인하고¹⁷

¹⁶ 아티클 19 조, 온라인 익명권, 노트 3, p.22-23.

¹⁷ 유엔 인권 이사회(2011), 유엔 특별 조사 위원에 언론 및 표현의 자유를 보호하고 촉진하는 것과 관련하여 제출된 보고서, 프랭크 라튀, 2011.03.16, A/HRC/17/27, 53 문단 (“사생활의 권리는 개인이 스스로의 의견을 자유롭게 표출하는데 매우 중요하다. 역사 속에서, 공적 영역에의 논쟁적 주제들에 대한 논의를 하고자 하는 의지는 항상 그것을 익명으로 할 수 있는지와 연결되었다.”), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

표현의 자유 침해요소와 마찬가지로 익명성을 침해하는 요소 역시 적법성, 필요성, 과잉금지의 원칙의 적용을 받아야 한다고 강조했습니다.¹⁸

13. 2013년에 라튀 특별보고관은 사생활의 자유와 표현의 자유가 서로 긴밀히 연결되어 있음을 다시 한번 강조하였고, “의사소통의 익명성, 보안성, 사생활 보호의 필요성을 지적하였습니다.”¹⁹

14. 라튀 특별보고관은 “인터넷의 출현으로 인해 가장 발전된 부분은 익명으로 정보에 접근, 정보를 교환할 수 있다는 것이지만 보안과 법집행의 명목으로 국가가 점차적으로 익명 커뮤니케이션의 기회를 없애고 있다” 고 이야기 했습니다.²⁰ 특별보고관은 특히 “ 뉴스 사이트, 블로그에 의견을 달거나 주요 웹사이트를 방문할 때, 혹은 휴대전화나 심카드를 구입할 때 등록이나 신분 증명을 요구하는 일이 증가하고 있다” 고 설명했습니다.²¹ 특별보고관은 익명성 제한이 생각과 정보의 자유로운 표현을 위축시킨다” 고 결론 내리며, 이것이 또한 “개인의 필수적인 사회적 관계로부터 단절을 초래하고, 표현과 정보의 자유를 위축시키며, 사회적 불평등을 심화시키는 결과” 를 초래할 수 있다고 말했습니다.²²

15. 현 유엔 특별보고관 데이빗 케이의 의견 역시 전임자의 권고와 다르지 않습니다. 케이 특별보고관도 표현의 자유와 사생활의 자유간의 상호연결성을 강조하였습니다.²³ 보고관은 익명성에 대한 간섭은 인권의 관점에서 해석되어야 하며²⁴, “기업들은 암호화와 익명성을 제한하는 기업정책들을 살펴야 한다”²⁵고 말했습니다. 마지막으로, 케이 특별보고관은 그러한 정책에 영향을 받을 경우

¹⁸ 상동, 24 문단, 49 문단.

¹⁹ 유엔 인권 이사회(2011), 유엔 표현의 자유 특별보고관의 보고서, 프랭크 라튀, 2011.04.17, A/HRC/23/40, 79 문단, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, (강조 포함).

²⁰ 상동, 47 문단.

²¹ 상동.

²² 상동, 49 문단.

²³ 유엔 인권이사회 (2015), 유엔 표현의 자유 특별보고관의 보고서, 데이빗 케이, 2015.05. 22. A/HRC/29/32, 16 문단,

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

²⁴ 상동, 31 문단 (“표현의 자유를 가능하게 하는 암호화와 익명성에 대한 제한은 잘 알려진 3 가지 기준을 만족시켜야 합니다: 표현에 대한 제한 법률로 규정되어야 한다; 적법한 근거에 의해서만 제한할 수 있다 (규약 19 조 3 항에 근거); 필요성과 과잉금지의 원칙에 따라야 한다.”).

²⁵ 상동, 60 문단.

적절한 구제조치가 있어야 하고, 사생활 침해 발생 시 해당 개인이 통지받을 수 있어야 의미있는 구제라고 역설했습니다.²⁶

16. 다른 유엔 특별 보고관들과 마찬가지로 미주인권위원회 표현의 자유 카탈리나 보테로 마리나 특별보고관도 2013년 보고서를 통해 사생활과 표현의 자유를 위한 익명성의 중요성에 관한 동일한 견해를 표명했습니다. 특별 보고관은 “대중의 활동이나 신분이 지목되거나 기록되지 않는 온라인상 공간의 증진이 필요” 하며 “표현의 자유 권리를 행사하기 위한 안전한 환경을 만드는 것이 국가의 역할인데 그렇지 않을 경우 자유로운 의사소통이 위축되고 방해받을 수 있다” 라고 지적했습니다.²⁷ 보고관은 또한 어떠한 상황에서는 법률에 따라 사법부가 금지된 활동을 하는 정보통신자에게 적절한 조치를 취할 수도 있다” 고 설명했습니다.²⁸

17. 유럽회의의 장관급 위원회는 2003년 온라인 통신의 자유에 대한 선언을 채택했습니다.²⁹ 선언의 일곱 가지 주요원칙 중 하나가 익명성에 관한 것입니다.

온라인 감시로부터 보호받고 자유로운 생각과 정보의 표현을 증진하기 위해 회원국은 신분을 밝히지 않고자 하는 인터넷 사용자들의 의사를 존중해야 한다. 이것은 회원국이 국내법, 인권과 기본적 자유의 보호에 대한 협약, 그리고 사법권과 경찰분야에 관한 국제적 합의 아래 범죄행위를 저지른 사람들을 추적하기 위한 조치를 취하거나 협력하는 것은 포함하지 않는다.

18. 위원회는 이 원칙을 뒷받침하는 해설에서 “익명으로 남고자 하는 사용자들의 의사를 존중하기 위해 가장 중요한 원칙” 이라고 설명했습니다.³⁰ 위원회는 “사용자들은 신분을 밝히지 않고 인터넷에 발언을 게재할 타당한 이유가 있을 수 있고, 신분을 밝히라고 요구하는 것은 사용자의 표현의 자유를 지나치게 제한하는 것” 이라고 했습니다.³¹ 또한 사용자는 영장을 발부받지 않고 온라인 감시를 하는 공공기관이나 민간기관으로부터 보호받을 필요가 있음을 역설했습니다.³²

²⁶ 상동, 18 문단.

²⁷ 미주인권위원회(2013), 인터넷에서의 표현의 자유, Catalina Botero Marina, 2013.12.31, OEA/Ser.L/V/II, 23 문단, http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20WEB.pdf.

²⁸ 상동, 135 문단.

²⁹ 유럽회의, 온라인 통신의 자유에 대한 선언(2013.03.28 840 회 차관회의의 위원회에서 채택됨), [http://portal.unesco.org/ci/en/files/25147/11861368651Declaration-Inf\(2003\)007.pdf/Declaration-Inf\(2003\)007.pdf](http://portal.unesco.org/ci/en/files/25147/11861368651Declaration-Inf(2003)007.pdf/Declaration-Inf(2003)007.pdf).

³⁰ 상동, p. 12.

³¹ 상동.

³² 상동.

19. 이후 유럽에서는 익명성과 익명 표현 대한 법의 태도가 확장되었고 개선되어 왔습니다. 유럽인권재판소가 Delfi AS v. Estonia. 사건에서 익명성과 관련하여 장관위원회의 2003년 선언을 고려한 것은 당연합니다. 법원은 온라인 발언에서의 익명성의 중요함을 재차 확인하였고, 인터넷 사용자들이 이용하는 다양한 익명성의 종류를 설명하였습니다. 또한 법원은 “이러한 정보의 노출은 수사당국 혹은 사법당국의 명령을 요구하며, 극히 제한된 조건하에서만 가능하다” 라고 판시하며, 개인식별정보의 노출을 방지할 수 있는 절차적 안전보호장치를 강조하였습니다.³³
20. 사생활과 표현의 자유를 보장하는 익명성과 그 역할을 공인하는 국제사회의 흐름에 맞추어 프라이버시 인터내셔널은 헌법재판소에 전기통신사업법의 83조 3항 83조 4항과 같이 익명성을 제한하는 법률을 국제 인권법제의 기준으로 심판해 주시기를 요청합니다.

C. 익명성과 전기통신사업법의 83조 3항 83조 4항이 가지는 상호작용성

21. 83조 3항에 의하여 전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함), 정보수사기관의 장이 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위해 정보수집을 요청하면 그 요청에 따를 수 있습니다.

22. 전기 통신 사업법은 ‘통신 자료’ 를 다음과 같이 정의합니다.³⁴

1. 이용자의 성명
2. 이용자의 주민등록번호

³³ Delfi AS v. Estonia, 신청번호 64569/09, 2015.06.16, 148 문단.

³⁴ 전기통신 사업법에서 “통신자료” 가 의미하는 것은 일반적으로 ‘가입자 자료’ 혹은 ‘가입자 정보’ 이다. 예를 들어 부다페스트 협약의 18조 3항에서는 ‘가입자 정보’ 를 아래와 같이 정의한다.

이 조에서 의미하는 가입자 정보란 컴퓨터 데이터의 형태로 또는 그 밖의 다른 형태로 포함되어 있는 모든 정보로써, 통신데이터나 내용 관련 데이터 (이외의 것으로)를 제외한, 서비스제공자의 서비스 이용자에 관한 것으로써 서비스제공자에게 보관되어 있고,

- a) 이용 중인 통신서비스의 종류, 이 서비스에 관련되는 기술적 조치 및 서비스의 기간;
- b) 가입자의 신원, 주소, 전화와 그 밖의 접속 번호, 통신 서비스와 관련한 계약이나 협약에 근거해서 이용될 수 있는 요금의 청구 및 지급에 관한 정보;
- c) 통신 서비스와 관련한 계약 또는 협정에 근거하여 존재하는 전기통신시설이 있는 장소에 관한 그 밖의 정보를 통해서 확정될 수 있는 모든 정보를 의미한다.

3. 이용자의 주소
4. 이용자의 전화번호
5. 이용자의 아이디
6. 이용자의 가입일 또는 해지일

23.83 조의 4 항은” 통신자료” 제공 요청은 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 하여야 하고, 서면으로 요청할 수 없는 긴급한 사유가 있을 때에는 제외한다고 규정합니다.

24. 전기통신사업법의 83조 3항과 4항은 익명성과 익명표현을 위태롭게 하고 사생활과 표현의 자유를 침해하는 일반적인 수단입니다. 표면적으로 이는 전기통신사업자에게 가입자 정보를 다양한 정부 기관에서 제출하는 서면 한 장에 넘길 수 있도록 전권 위임을 제공합니다. 위에서 논의하였듯이 정부에 가입자 정보를 제공함으로써 회사는 개인 식별 정보를 다른 인적 자료와 함께 묶을 수 있고, 이는 사생활과 표현의 자유의 심각한 침해를 야기합니다.³⁵

25. 한국에서 이러한 침해는 방대하게 일어나고 있습니다. 미래창조과학부의 2016년 보고서에 따르면 정부기관은 2015년 10,577,079 개의 통신기기로부터 가입자 식별 정보와 5,484,945 건의 통신자료에서 메타데이터 기록을 수집했습니다.³⁶ 이러한 정보를 서로 연결함으로써, 한국정부는 쉽고 효율적으로 수백만 국민들의 상세한 프로파일을 작성할 수 있습니다.

D. 표현의 자유와 사생활의 권리를 침해하는 전기통신사업법의 83조 3항과 83조 4항

26. 형사 사건이나 국가 안보에 중대한 위협에 대응하기 위해 표현 및 사생활의 자유에의 일정한 제약이 필요하다는 것은 이미 잘 정립된 이론입니다. 그러나 감시는 이러한 권리를 침해하는 것이기에, 반드시 목적의 합법성, 필요성,

³⁵ 국제 데이터 보호 기준은 가입자 자료가 곧 개인 정보임을 인정한다. 예를 들어 EU 개인정보보호지침의 4 조는 개인정보를 “식별되거나 식별가능한 자연인에 관한 정보” 라고 이야기하고, ‘식별 가능한 자연인’ 을 ‘직접 또는 간접적으로 특히 식별 번호 또는 자신의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 신원에 특정적인 하나 이상의 요소를 참조하여 식별될 수 있는 자’ 라고 이야기한다. 동 지침 4(1). 수집과 공개를 포함한 가입자 자료의 처리는 안전보장조치의 대상이 될 수 있고, 되어야 한다.

³⁶ 해당보고서는 미래창조과학부 웹사이트에서 확인가능,
<http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1316113&snsMIId=NzM%3D&getServerPort=80&snsLinkUrl=%2Fweb%2FmsipContents%2FsnsView.do&getServerName=www.msip.go.kr>.

과잉금지의 원칙 등이 적용되어야 합니다. Article 19가 헌법재판소에 밝힌 이유와 같이 전기통신사업법의 83 조 3 항과 83 조 4 항은 이러한 요건을 충족시키지 못합니다.³⁷

27. 또한 전기통신사업법의 83 조 3 항과 83 조 4 항은 국제인권 기준에 부합하는 추가적인 안전보장장치를 결여하고 있습니다. Article 19의 서면은 두 가지 안전보장장치를 강조합니다. (1) 전기통신사업자에게 가입자 정보를 요청할 때, 국가가 영장을 발부 받도록 하는 것과 (2) 정부에게 제출된 가입자 정보의 당사자에게 통지를 하도록 한 것입니다.
28. 프라이버시 인터내셔널은 정부가 한국 가입자 정보에 접근하는 것을 통제 할 효과적인 안전보장장치의 필요성과 Article 19의 분석을 지지할 추가적인 기관의 필요를 주장합니다.

1. 독립된 사전 허가

29. 프라이버시 인터내셔널은 EU 사법재판소의 최근 두 가지 사건에 주목합니다. 이 판결은 정부가 전기통신사업자가 보유한 통신 자료에 접근하기 앞서 독립된 허가 절차를 거치는 것의 중요성을 이야기 하고 있습니다. 프라이버시 인터내셔널은 이 판례가 통신 자료가 아닌 가입자 정보에 대한 사건임을 인지하고 있습니다. 그러나 정부가 가입자 정보, 특히 통신 자료와 결합한 가입자 정보에 접근할 때 제기되는 익명성(사생활과 표현의 자유를 포함)의 중요성으로 인해 이와 유사한 안전보호장치는 필요합니다.
30. 디지털 라이츠 아일랜드 케이스에서 EU 사법재판소 대법원은 전기통신사업자가 심각한 범죄의 예방 및 탐지를 위해 이용자 통신 자료를 최대 2년간 묶음으로 보관하도록 규정한 2006년 EU의 데이터 보유지침이 사생활의 자유와 유럽연합 기본권 헌장에 규정된 7 조와 8 조의 권리를 침해한다고 판시하였습니다.³⁸ EU 사법재판소는 이 지침이 보유한 데이터를 이용하고 접근하는데 있어 충분히 절차적·실질적인 안전보호장치를 포함하지 않았음을 지적했습니다. 판결은

³⁷ 아티클 19 조 제삼자의견서, 2016 헌마 388, 대한민국 헌법재판소, 2016.12.15 판결, pp. 6-10.

³⁸ 법원 판결 (대법원), Digital Rights Ireland Ltd v Minister for Communications et al (C-293/12 and C-594/12), CJEU, 2014.04.08, (<http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=40531>).

“관할 국가기관의 접근이 법원이나 독립된 행정기관의 사전 검토에 따라 이루어지지 않았음”³⁹을 강조했습니다.

31. 전기통신사업자가 심각한 범죄의 예방 및 탐지를 위해 이용자의 통신 자료를 묶음으로 보관하도록 의무화한 스웨덴과 영국의 법(스웨덴의 경우 6개월, 영국의 경우 1년)에 대해 논의한 텔레 2 스베리에 에이비, 톰 왓슨 외 사건에서, EU 사법재판소 대법원은 아래와 같이 판시하였습니다.

원칙적으로 관할 국가기관이 정보를 획득하고자 할 때는, 위급함이 유효하게 인정되는 경우를 제외하고 법원이나 독립된 행정조직의 사전 검토의 적용되며, 이러한 법원이나 독립된 행정 조직의 결정은 당국의 합리적 요청, 특히 범죄의 예방, 탐지 및 기소의 절차적 체계에 의거하여 만들어져야 한다.⁴⁰

32. 이러한 결정은 가입자 정보에 대한 접근을 허용하는 몇몇 국가들의 방식과도 상응합니다. 사이버범죄협약위원회 평의회의 2014년 연구에 따르면 절반이 넘는 회원국이 “가입자 정보의 획득은 사법적 결정에 의해 이루어 져야 한다”고 규정하고 있습니다.⁴¹

33. 2014년 캐나다 대법원은 알 v. 스펜서 판결에서 “사생활 자유의 범익은 무분별한 압수수색으로부터의 헌법의 보호와 이와 연결된 사생활 자유의 범익의 중요성”을 적시했습니다.⁴² 판결은 경찰의 정보 감별 요청이 “개인이 익명으로 수행한 온라인 활동, 법원이 중대한 사생활 보호의 이익을 가지는 것으로 인정한 활동과 용의자를 연결 하여 사생활 자유의 익명성과 관련된다”고 결정했습니다.⁴³ 법원은 가입자가 자신의 식별 정보에 대한 사생활로 보호될 것에 대한 합리적 기대를

³⁹ 상동, 62 문단.

⁴⁰ 법원 판결 (대법원), Tele2 Sverige AB and Tom Watson & Others (C-698/15), CJEU, 2016.12.21, 120 문단, (<http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=40531>).

⁴¹ 사이버범죄방지협약위원회, 유럽의회, 가입자 정보 취득에 관한 규칙, 2014.12.03, p.28, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1>.

⁴² R. v. Spencer, 2014 SCC 43, 48 문단, (<http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do>).

⁴³ 상동, 50 문단.

가지고 있고,⁴⁴ 따라서 향후 경찰은 유사 상황에서 법원 명령을 확보하여야 한다고 아래와 같이 판시하였습니다.

이 사건을 전체적으로 보면 가입자 정보가 사생활로 지켜질 것에 대한 합리적 기대가 존재합니다. 이러한 정보의 노출은 온라인 상 민감하고 사적인 활동을 이용자의 신원이 통상적으로 익명으로 머물 것이라는 기대에 기반한 활동입니다. 경찰관의 ISP로 하여금 자발적으로 이러한 정보를 제공하도록 한 것은 수색에 해당합니다.⁴⁵

34. 또한 프라이버시 인터내셔널은 표현의 자유를 행사함에 있어 익명성의 중요성에 대해 역설하였던 유엔 특별보고관 케이의 2015년 보고서를 주목합니다. 이 보고서에서 특별보고관은 다음과 같은 사항을 특별히 권고하였습니다.

국가는 사상과 표현의 자유 및 사생활의 자유에 대한 권리를 보호하고 증진시키기 위한 법률과 규정을 개정하거나 설립하여야 한다. 암호화와 익명성과 관련하여 국가는 무규제의 원칙이나 포괄적인 보호 정책을 도입하여야 하고, 개별사건의 관한 규제와 수단의 적법성, 필요성, 법익의 균형성, 목적의 정당성에 입각하여 *별개의 법원 명령을 통해서만 이루어 져야 합니다*...⁴⁶

35. 따라서 유엔 자유권규약 위원회는 “전기통신사업법 83조 3항에 의하면 가입자 정보는 전기통신사업자에게 수사의 목적을 위해 영장 없이 요청 가능하다”는 점에 우려를 표명했습니다.⁴⁷ 위원회는 국가에 “가입자 정보는 오직 영장에 의해서만 제출” 되도록 정부에 권고했습니다.⁴⁸

2. 사용자 통지

36. 전기통신사업법은 정부가 가입자 정보에 접근할 시 이용자에게 그 사실을 통지할 의무를 규정 하고 있지 않습니다.

⁴⁴ 상동, 62 문단.

⁴⁵ 상동, 문단 66.

⁴⁶ 유엔인권이사회(2015), 특별 보고관 케이의 보고서, 노트 23, 57 문단.

⁴⁷ 자유권규약 인권위원회, 대한민국 4차 정례보고 최종견해, 유엔 문서 CCPR/C/KOR/CO/4, 2015.12.03, 42 문단.

⁴⁸ 상동, 43 문단.

37. 텔레 2 스페리에 에이비, 톰 왓슨 외 사건에서, EU 사법재판소는 다음과 같이 판시했습니다.

마찬가지로, 수집된 정보에 접근하는 관할 당국은 접근에 대한 통지가 진행 중인 수사에 위태롭지 않게 되는 즉시 당사자에게 국내법 절차에 따라 통지해야 합니다. 이러한 통지는 당사자가 침해된 권리에 대한 법적 구제를 포함한 개인의 권리를 행사하는데 필수적입니다.⁴⁹

38. 이러한 EU 사법재판소의 접근은 전 유엔 특별보고관 라튀의 2013년 보고서에 포함된 다음의 권고를 반영하고 있습니다.

개인이 국가의 통신 감시의 대상이 되었거나 통신의 기록이 열람된 경우 이에 대한 통지를 받을 법적 권리를 가집니다. 감시 전 혹은 감시 중 통지는 효과적인 감시를 위태롭게 할 수 있다는 점이 인정됩니다. 그럼에도 불구하고 감시가 종료되고 난 후 통지되어야 하며 당사자가 사후에 통신정보 사용에 관한 배상을 청구할 기회가 주어져야 합니다.⁵⁰

39. 유엔 특별 보고관 케이 역시 2015년 보고서에서 다음과 같이 이야기했습니다.

개인과 시민사회는 국가와 비국가 행위자에 의해 방해받고 공격당하고 있는데, 암호화와 익명성은 이에 대한 보호를 제공해 줄 수 있습니다. 시민·정치적 권리에 관한 국제규약의 17조 (2)에 의하면, 국가는 자의적이거나 불법적인 간섭 및 공격으로부터 사생활을 보호할 의무가 있습니다. 이 의무에 따라 국가는 정부 혹은 비정부 행위자의 자의적이고 불법적인 간섭 및 공격으로부터 사생활을 보호할 국내 법률을 마련해야 할 필요가 있습니다. 이러한 보호는 불법행위에 대한 배상을 포함해야 하고 보상받을 권리가 실효성을 가지기 위해 개인은 약화된 암호화나 강제 사용자 정보 공개 등 모든 사생활 침해에 관한 통지를 받아야 합니다.⁵¹

IV. 결론

⁴⁹ 텔레 2 스페리에 에이비, 톰 왓슨 판결문, 노트 40, 문단 121.

⁵⁰ 유엔 인권이사회(2013), 특별 보고관 케이의 보고서, 노트 19, 82 문단.

⁵¹ 유엔 인권이사회(2013), 특별 보고관 케이의 보고서, 노트 19, 82 문단(부분강조 포함).

40. 앞서 논의한 바와 같이 프라이버시 인터내셔널은 전기통신 사업법의 83 조 3 항과 83 조 4 항이 대한민국이 이행의무가 있는 국제 인권법과 부합하지 않는다고 주장합니다. 프라이버시 인터내셔널은 헌법재판소가 논의된 기준을 고려하여 해당 법률의 위헌여부를 심판할 것을 촉구합니다.

캐롤라인 윌슨 펠로
법률고문

토마소 펠체타
법무담당관

스칼렛 김
법무담당관

프라이버시 인터내셔널
62 브리튼 스트리트
런던 EC1M 5UY, 영국
Tel: +44 20 3422 4321
caroline@privacyinternational.org