의 견 서

사 건 서울중앙지방법원 2015고합665 개인정보보호법위반 등
피고인 재단법인 약학정보원 외 12인
제출자 1. 진보네트워크센터
2. 경실련 시민권익센터
3. 건강권실현을 위한 보건의료단체연합 (건강사회를위한약사회 건강사회를위한치과의사회 노동건강연대 인도주의실천의사협의회 참의료실현청년한의사회)

위 제출자들은 오랜 기간 동안 개인정보보호법의 제정을 위해 노력해 왔으며 개인정보보호법 제정 이후에 올바른 개인정보보호제도의 정착을 위한 활동해 왔습니다. 제출자들은 우리 사회의 개인정보보호제도에 중요한 영향을 미칠 수 있는 위 사건에 관하여 올바른 판단이 내려지기를 바라는 마음에서 다음과 같은 의견을 제시합니다.

1. 본 사안의 중요성 - 의견을 제시하는 이유

개인정보범죄 정부합동수사단은 2015년 7월 다국적기업인 한국아이엠에스헬스(이하 '한국IMS'라 합니다.)가 2011년부터 2014년까지 우리나라 국민 4,399만명의 의료정보 약47억건을 약20억원에 불법적으로 사들여 이를 본사에 보내 재가공한 후 국내 제약회사에 약100억원에 되팔았다는 수사결과를 발표하였고, 국민들은 이 소식에 커다란 충격을 받았습니다. 국민들은 이름도 모르는 외국 기업에 자신의 건강정보가 제공된다는 것은 꿈에도 생각하지 못했기 때문입니다.

더욱 놀라운 것은 국민들이 전혀 모르는 외국 기업에 건강정보가 제공된 데에 약국의 환자정보를 취합한 (재)약학정보원과 병원의 요양급여청구 프로그램을 통해 병원의 환자정보를 취합한 의료정보시스템 회사(이하 '지누스'라 합니다)가 관여했다는 점입니다. 이렇듯 거의 모든 국민의 개인정보를, 그것도 민감정보인 건강에 관한 정보를 불법으로 취득하고 이를 외국 기업에 판매한 본 사안에 대해서는 당연히 엄중한 처벌이 이루어져야할 뿐만 아니라,

해당 개인정보를 실질적으로 파기하도록 하는 조치까지 취해져야 동일한 위법행위가 반복되지 않을 것입니다.

그런데 언론보도에 의하면, 한국IMS, 약학정보원, 지누스 등(이하 포괄하여 '피고인들'이라고 합니다.)은 식별정보를 암호화하였으므로 개인을 식별할 수 없는 정보로 개인정보가 아니라는 주장을 하고 있다고 하며, 나아가 본 사안은 21세기의 원유라 할 수 있는 빅데이터 산업과 직결된 사안으로 자신들의 행위를 위법하다고 할 경우 의료정보의 통계처리를 통한 의약학의 발전을 저해함을 물론이고 우리나라의 새로운 먹거리인 빅데이터 산업의 싹을 자르는 결과가 될 것이라고 주장하고 있다고 합니다.

하지만, 아래에서 보다 구체적으로 살펴보는 바와 같이 개인정보의 암호화는 개인정보의 식별성을 제거하는 수단이 아닌 개인정보의 안전성을 확보하는 수단에 불과하고, 식별정보 또는 식별가능정보가 포함된 건강정보의 거래는 빅데이터 산업과도 무관하다는 점에서 피고인들의 주장은 잘못된 것입니다.

그런데, 피고인들의 위 주장은 최근 정부가 일방적으로 추진하고 있는 빅데이터 산업 진흥의 논리에 기대고 있는데다, 개인정보보호와 산업발전 사이에 균형을 유지해야 하는 정부가 법률적 근거가 없고 국제적 기준에도 부합하지 않은 '비식별화 가이드라인'을 만드는 등 일방적으로 산업계의 이익만 대변하고 있는 것도 현실이어서, 우리 시민단체는 이런 현실과 이런 현실에 기대고 있는 피고인들의 행태를 크게 우려하고 있습니다.

이에 본 사안에서 올바른 판단이 내려져 개인정보보호와 빅데이터 산업 발전 사이에 균형이 유지되고, 익명화 내지 비식별화 조치의 법적 의미 등이 분명히 제시되어 더 이상의 불필요한 사회적 논란이 일어나지 않도록 하기 위하여 이 의견서를 제출하게 되었습니다.

다만, 우리 시민단체는 이 의견서를 통해 피고인들에 대한 전체 공소사실에 대한 법률적 분석의견을 드리고자 하는 것은 아니므로, 이하에서는 개인정보 암호화와 빅데이터 산업의 문제에 관한 의견만을 간략하게 제시하고자 합니다.

2. 개인정보보호법의 일반 원리와 본 사안의 쟁점

가. 개인정보보호법의 일반 원리

2011년부터 시행되어 온 우리나라 개인정보보호법(이하 단순히 '법'이라고 하는 경우는 개인정보보호법을 의미합니다.)에 의하면, 업무를 목적으로 개인정보파일을 운용하는 '개인정보처리자'는 살아있는 개인에 대한 식별가능한 정보('개인정보')를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등의 '처리'를 하고자 할 때에는 개인정보보호법이 정한 기준에 따라 개인정보를 수집하고, 이용하거나, 제3자에게 제공해야 합니다.

개인정보보호법은 개인정보의 수집과 이용의 기준에 관하여는 제15조에서, 수집한 개인정보를 수집의 목적범위 내에서 제3자에게 제공하는 기준에 관하여는 제17조에서, 수집의 목적범위를 초과하여 이용하거나 목적범위를 초과하여 제3자에게 제공하는 기준에 관하여는 제18조에서 규정하고 있습니다.

요컨대, 우리나라 개인정보보호법은 개인정보의 '처리'를 크게 ①개인정보의 수집과 이용, ②목적 내 제3자 제공, ③목적 외 이용(목적 외 제3자 제공 포함)으로 구분하여 규율하고 있다고 볼 수 있습니다. 구체적으로 제15조는 개인정보의 수집과 이용에 관하여 6가지의 적법 요건을, 제17조는 개인정보의 목적 내 제3자 제공에 관하여 4가지의 적법 요건을, 제18조는 개인정보의 목적 외 이용(목적 외 제3자 제공 포함)에 관하여 9가지의 적법 요건을 규정하고 있으며, 이 적법 요건을 충족하지 못하는 개인정보의 수집, 이용, 제공 행위는 개인정보보호법을 위반하는 위법한 행위입니다.

개인정보보호법은 '처리'의 개념을 규정하고 있을 뿐 '이용'의 개념을 따로 규정하고 있지 않으나, 제3장에서 '개인정보의 처리'라는 제목을 둔 후, 제1절에서 개인정보의 '수집, 이용, 제공 등'이라고 규정하고, 제1절의 하위 규정인 제15조 내지 제22조에서 수집, 이용, 제공의 행위만을 규정하고 있으므로, 개인정보보호법 제1절 제15조 내지 제22조에 규정된 '이용'이란 "수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등"의 '처리' 개념에서 수집과 제공을 제외한 나머지의 모든 행위 양식을 포괄하는 의미로 해석됩니다.

이에 따라 개인정보처리자는 목적을 특정하여 개인정보를 수집하여야 하며 수집한 개인정보를 해당 목적의 범위 내에서 '이용'할 수 있고, 법 제17조와 법 제18조에 규정된 적법 요건을 충족하는 범위 내에서만 개인정보를 제3자에게 제공하거나, 그 목적 범위를 초과하여 이용 또는 초과하여 제3자에게 제공할 수 있습니다.

또한 수집한 개인정보 중 식별정보를 제거하거나 다른 정보로 대체하여 특정 개인을 알아볼 수 없는 형태로 가공[1]하고자 하는 경우에도 그것은 '가공, 편집 등'의 '이용' 행위에 해당되므로, 법 제15조 제1항 각호의 적법요건(정보주체의 동의, 법률의 특별규정, 공공기관의 소관업무 수행, 정보주체 또는 제3자의 급박한 이익, 개인정보처리자의 정당한 이익 등) 중 하나를 충족해야 가능합니다. 다만, 특정 개인을 알아볼 수 없는 형태로 개인정보를 가공하는 것은 정보주체의 이익에 반하지 않으며 개인정보처리자에게도 그렇게 처리할 정당한 이익이 있는 경우가 있을 수 있으므로, 일정한 조건 하에 개인정보를 익명으로 가공하는 행위는 법 제15조 제1항 제6호에 따라 "개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우"에 해당하여 허용되는 경우가 있을 것입니다. (따라서 우선 본 사안의 식별정보를 암호화하여 식별성이 제거되었다고 하며 개인정보보호법 위반이 아니라는 피고인들의 주장은 그 자체로 타당하지 않습니다. '식별정보의 암호화' 행위 자체의 적법요건을 충족하였다고 보기 어렵기 때문입니다. 피고인들은 수집 당시부터 '익명정보'인 경우와 '식별정보의 익명화 처리' 또는 '식별정보의 비식별화 처리'의 경우를 혼동하고 있습니다. 수집 당시 식별정보를 이후 일정하게 가공 처리하는 모든 행위는 개인정보보호법의 규율 대상입니다.)

한편, 개인정보보호법은 제23조에서 건강 등에 관한 개인정보를 민감정보로 분류하고 다른 개인정보의 처리에 대한 동의와 별도의 동의를 받거나, 법령에서 민감정보의 처리를 요구 또는 허용하는 경우에 한하여 민감정보를 처리할 수 있도록 허용하고 있습니다. 법 제23조는 제1항 제1호에서 제17조를 인용하고 있으므로, 민감정보에 대해서도 법 제17조의 적법요건에 해당하는 경우에는 '목적 범위 내의 제3자 제공'이 가능할 것이나, 수집목적의 범위를 초과(목적 초과의 제3자 제공 포함)하는 이용에 관한 법 제18조가 적용되는지는 불분명합니다.

---

1) 보통 익명화 조치 또는 비식별화 조치라고 칭하는 행위를 말합니다. 우리 개인정보보호법은 제18조 제2항 제4호에서 "특정 개인을 알아볼 수 없는 형태"라는 규정을 두고 있으므로, '익명화' 조치라는 용어를 사용하는 것이 법에 더 부합하는 용어 사용일 것으로 보입니다.

법 제23조의 적용을 배제하고 있는 법 제58조 제1항에 따라 통계법, 국가안전보장, 공중위생 등에 필요한 경우에 민감정보를 처리할 수 있는 예외가 있기는 하나, 민감정보의 경우에도 법 제18조 제2항에 규정된 범죄 수사의 필요, 법원의 재판업무에 필요한 경우가 있을 수 있다는 지적이 가능하다는 점에서, 민감정보에도 법 제18조가 적용된다는 해석[즉, 민감정보도 법 제18조의 적법요건을 충족하는 경우 목적 외 이용(목적 외 제3자 제공 포함)도 가능하다는 해석]을 해야 한다는 주장이 제기될 수 있습니다. EU는 우리의 민감정보에 해당하는 사상, 종교, 건강에 관한 개인정보("special categories of data")의 처리를 금지하면서도, 정보주체의 동의, 고용관계, 정보주체나 제3자의 중대한 이익, 공개된 정보, 헬스케어나 치료의 제공에 필요, 범죄나 형사판결과 관련되는 경우 등의 사유가 있을 경우에는 그 처리를 허용하고 있습니다. (EU의 현행 규정인 개인정보보호지침[2] 제8조 및 2018년 시행예정인 개인정보보호규정[3] 제9조 참조. GDPR은 제9조에서 민감정보의 처리를 허용하는 위와 같은 예외 사유 외에 '과학적, 역사적 연구나 통계를 위한 처리에 필요한 경우'의 사유를 예외 사유로 추가하고 있습니다.)

나. 본 사안의 쟁점

본 사안의 경우 개인의 식별정보를 포함하는 병의원/약국의 처방/조제에 관한 개인의 민감정보의 최초 수집자인 병의원과 약국은 수집한 개인건강정보를 크게는 질환의 치료 목적, 작게는 처방이나 조제 목적 및 부수적으로 건강보험의 처리 목적으로 이용할 수 있고, 이러한 목적 범위 내의 이용을 위해 해당 정보를 약학정보원이나 지누스에게 제공할 수 있으나, 그러한 제공은 법 제17조의 적법 요건을 충족해야 합니다.

그런데, 병의원/약국 또는 약학정보원/지누스가 환자들로부터 개인건강정보를 수집하는 '목적 범위 내의 제3자 제공'에 관한 동의를 받았을 것으로 보이지 않으며, 달리 법 제17조 제1항 제2호의 적법 요건(법률의 특별한 규정,

---

2) 통상 Data Protection Directive("DPD")라 칭함. (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

3) 통상 General Data Protection Regulation("GDPR")이라 칭함. (Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

공공기관의 소관업무 수행, 정보주체의 급박한 생명 등 이익에 필요)을 충족하는 것으로 보이지도 않으므로, 병의원/약국이 개인건강정보를 약학정보원이나 지누스에 제공한 행위는 개인정보보호법 위반일 가능성이 높아 보입니다[4].

설사 병의원/약국의 약학정보원/지누스에 대한 개인건강정보의 제공이 적법하다고 하더라도, 약학정보원과 지누스가 병의원/약국으로부터 수집한 개인건강정보를 의약품의 마케팅 목적으로 개인의 진료 및 처방/조제정보를 수집하는 한국IMS에게 제공하는 것은 그 수집의 목적 범위를 초과하여 제3자에게 제공하는 것이므로, 법 제18조가 민감정보의 경우에도 적용된다는 해석에서만 가능한 행위인데, 개인정보보호법이 제23조에서 민감정보를 목적 범위를 초과하여 제3자에게 제공할 수 있다고 분명하게 규정하고 있지 않은 이상, 위 행위는 일단 개인정보보호법을 위반하는 행위로 볼 수밖에 없습니다.

설사 법 제23조의 민감정보 처리에도 법 제18조를 준용할 수 있다고 해석하는 경우에도, 약학정보원과 지누스가 개인건강정보를 한국IMS에 제공하는 것이 적법하기 위해서는 법 제18조 제2항의 적법 요건을 충족해야 하고, 피고인들의 주장은 주로 이 부분에 관한 것으로 보이므로, 아래에서는 피고인들의 행위가 법 제18조 제2항의 요건에 해당되는지 여부를 중심으로 살펴보겠습니다.

한편, 피고인들이 하고 있는 주민등록번호의 암호화 및 빅데이터 산업의 진흥에 필요하다는 주장은 모두 법 제18조 제2항 제4호의 "통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우"에 해당한다는 주장으로 보이며, 법 제18조 제2항 제4호 외의 나머지 적법 요건들 중 피고인들에게 해당할만한 규정은 없는 것으로 보이고, 정보주체의 별도 동의를 받지 않았다는 점은 피고인들이 모두 인정하고 있을 것이므로, 본 사안에서는 법 제18조 제2항 제4호의 해당 여부만 살펴보아도 무방해 보입니다.

따라서, 이하에서는 법 제18조 제2항 제4호의 해석 기준과 빅데이터 산업 사

---

4) 논의를 단순화하기 위하여 약학정보원/지누스에 대한 개인정보 제공의 적법성 문제는 이 정도로 약술하겠습니다.

이의 관계를 기준으로 피고인들 주장의 타당성을 살펴본 후, 피고인들의 또 다른 주장인 암호화된 주민등록번호의 식별성 문제를 살펴보겠습니다.

3. 법 제18조 제2항 제4호와 한국의 빅데이터 산업

가. 법 제18조 제2항 제4호와 한국의 빅데이터 산업

민감정보의 경우에도 법 제18조가 적용된다고 해석할 경우, 민감정보의 개인정보처리자(본 사안의 경우 약학정보원과 지누스)는 특정한 목적(본 사안의 경우 질환 치료 및 처방/조제 목적 등)을 위해 수집된 개인건강정보도 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우 특정 개인을 알아볼 수 없는 형태로 가공하여, 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공할 수 있을 것입니다.

민간정보 외의 사례이기는 하나, 최근 서울시에서 심야시간대의 이동인구가 많은 지역을 파악하여 심야시간대의 장거리버스노선을 결정하였는데, 이러한 결정은 이동통신사가 이동통신 이용정보를 기초로 심야시간대 유동인구 밀집도를 분석하여 통계로 작성한 후 서울시에 제공하였기에 가능한 일이었으며, A라는 회사는 비씨카드사의 신용카드사용 트래픽 데이터와 소상공인진흥원의 소상공인 정보 중 점포별 개폐업이력 정보 및 인구와 가구세대에 관한 공공 오픈데이터를 함께 가공하여 소상공인 창업지원을 위한 점포평가 서비스를 제공하고 있으며, 개인식별정보가 포함된 교통카드 이용내역을 바탕으로 한 통계정보를 기초로 상권분석정보가 제공되기도 하는데(빅데이터 분석활용센터, “창조경제 실현을 위한 2013 빅데이터 국내 사례집”), 이러한 일은 모두 법 제18조 제2항 제4호의 규정을 근거로 ‘통계 작성에 필요하여 특정 개인을 알아볼 수 없는 형태’로 제공하는 경우이기 때문에 가능한 일입니다.

즉, 우리 개인정보보호법은 위와 같이 산업적 필요에 의한 빅데이터 처리를 가능하게 하는 규정을 두고 있으며, 개인정보보호제도에 관하여 세계적인 기준을 선도하고 있는 EU의 경우에도 빅데이터 산업에 관하여 우리 법보다 특별히 더 허용적인 규정을 두고 있는 것도 아니므로, 빅데이터 산업 발전이 필요하다는 논리로 우리 개인정보보호법의 한계를 지적하는 비판은 타당하다고 할 수 없습니다.

즉, EU는 1995년의 개인정보보호지침(Data Protection Directive[5])에서 역사적, 통계적 또는 과학적 목적으로 개인정보를 추가 처리하는 것(further processing[6])이 적절한 보호장치가 부여되어야 한다는 조건하에 허용된다고 규정하고 있을 뿐이며(전문 제29호[7], 제6조 제1항 b호[8]), 위 Directive를 대체하는 법률로 2016년에 제정되었으며 개인정보보호제도에 관하여 광범위하고 세세한 규정을 담고 있는 일반정보보호규정(General Data Protection Regulation[9]도 가명화 조치(pseudonymization)를 취할 경우 추가 처리(further processing)를 더 쉽게 허용하는 규정(GDPR 제6조 제4항)을 두는 외에 공익 목적의 아카이빙, 과학이나 역사 연구 또는 통계적 목적으로 개인정보를 추가 처리(further processing)하는 것을 허용하고 있을 뿐입니다(GDPR 제5조 제1항 b호[10]).

---

5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

6) 우리 법의 '목적 외 이용'과 유사한 개념. 다만 문자 그대로의 뜻으로는 '수집 목적에 부합하는(또는 양립가능한) 추가처리'의 의미이므로, 수집 목적과 관련성을 요구하지 않는 우리 법 상 '목적 외 이용' 보다는 좁은 개념으로 보아야 하겠습니다.

7) "(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual"

8) **Article 6**

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(이하 생략)

9) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data

10) **Article 5**

Principles relating to processing of personal data

1. Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(이하 생략)

오히려 EU 법은 수집 목적에 부합하는 또는 양립가능한 이용(compatible use)에 한하여 목적 외 이용(further processing)을 허용하고 있으나, 우리 개인정보보호법은 일정한 적법 요건을 충족하기만 하면 최초 수집 목적에 부합하는 목적인지 여부를 묻지 않고 목적 외 이용을 허용한다는 점에서 EU 법보다 넓은 범위에서 목적 외 이용을 허용하고 있다고 볼 수 있습니다.

우리 개인정보보호법의 한계를 지적하는 논자는 대부분 미국의 사례를 주요한 근거로 제시합니다.

하지만, 개인정보에 관한 개인의 통제권이 헌법적 기본권이며 EU 인권헌장(The Carter of Fundamental Rights of the EU)에 규정되어 있는 EU의 경우[11]와 미국의 법 체계는 근본적으로 다르며, 미국의 법 체계는 우리 법 체계와도 크게 다르므로, 미국의 사례는 우리 법 해석과 체계 구성에 참고하기 어렵습니다.

즉, 미국에서 개인정보에 관한 권리는 헌법적 권리가 아니며 단지 불법행위법(tort law)에 의해 보호되는 제한적인 것이고, 개별 분야의 개인정보를 규율하는 개별법이 있는 경우에 한하여 해당 개별법의 기준에 따라서만 보호되며[12], 개별법에 의해 규제되지 않은 행위는 원칙적으로 모두 허용되는 법 구조를 갖고 있습니다. 따라서 미국에서는 적법한 개인정보의 수집(정보주체의 동의나 개별법에 의한 수집 등) 이후의 처리(processing)에 아무런 규제가 없어, 미국의 개인정보처리자는 거의 아무런 제한 없이 자유롭게 다양한 내용과 형식의 개인정보 빅데이터를 처리할 수 있으며, 나아가 빅데이터를 기초로 하여 개인의 성향을 파악하는 프로파일링(profiling), 데이터 브로커에 의한 개인정보 데이터베이스의 거래가 모두 허용되는 상태[13]에 있으므로[14],

---

11) EU 인권헌장 제8조

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

12) 정부 부분의 개인정보에 관하여는 Privacy of 1974, 신용정보에 관하여는 Fair Credit Reporting Act of 1970, 의료정보에 관하여는 Health Insurance Portability and Accountability Act of 1996 등의 법률이 있습니다.

13) Federal Trade Commission, Data Broker: A Call for Transparency and Accountability, 2014

14) 이런 이유로 오바마 행정부는 2012년 2월에 “네트워크로 연결된 세계에서 소비자의 개인정보보호

개인정보자기통제권이 헌법적 권리인 우리나라의 경우에 참고할만한 사례라 할 수 없고, 오히려 EU의 기준이 우리의 법체계와 법감정에 부합한다고 하겠습니다.

나. "특정 개인을 알아볼 수 없는 형태"의 의미

법 제18조 제2항 제4호의 쟁점은 "특정 개인을 알아볼 수 없는 형태"가 무엇인지에 있습니다.

'개인정보'란 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)를 의미하므로, "특정 개인을 알아볼 수 없는 형태"란 표준개인정보보호지침 제8조 제4항이 규정하고 있는 바와 같이 "다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태"를 의미하는 것이며(행정안전부, 개인정보호보법령 및 지침고시 해설서 108쪽), '식별가능성'이 개인정보의 가장 중요한 개념이라는 점에서 볼 때는 '식별가능하지 않은 형태'를 의미한다고 볼 수 있습니다.

"통계작성의 목적"이라는 문구에 비추어 보아도 같은 해석을 도출할 수 있습니다. 통계작성, 통계처리란 집단현상을 숫자로 나타내는 것이므로, 그 집단을 구성하는 개별개체를 의미하는 '통계단위'는 개별적으로 식별할 수 없어야 함은 당연합니다. 즉, 일반적으로 통계수치나 통계결과를 통해 (다른 정보와 결합하더라도) 통계단위(통계 집단을 구성하는 개별개체)를 재식별해 내는 것은 가능하지 않거나 무척 어려운 일일 것이므로, "특정 개인을 알아볼 수 없는 형태"란 식별가능한 개인정보를 가공처리한 후에는 재식별의 가능성이 없거나 무척 낮은 정도까지 처리되어야 하는 것을 의미하는 것으로 볼 수밖에 없습니다.

수집 목적에 부합하는 추가 처리(further processing) 및 공익 목적의 아카이빙, 과학이나 역사적 연구 또는 통계 목적의 추가 처리(further processing)만을 허용하고 있는 EU 법의 해석도 마찬가지입니다.

(Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global digital Economy)"라는 보고서를 통해 소비자의 프라이버시권리를 더욱 적극적으로 보호해야 한다고 지적하였으며, 이를 실행하기 위해 2015년에 "Consumer Privacy Bill of Rights Act"를 발의하였으나, 아직도 이 법률은 미국 연방의회에서 통과되지 못한 상태입니다.

일반개인정보보호규정(GDPR)은 전문 26호에서 '익명의 개인정보'에는 개인정보보호규정이 적용되지 않는데, '익명 개인정보'란 '더이상 식별가능하지 않은'(no longer identifiable) 정보를 의미한다고 규정하여[15] '익명화 조치'(Anonymisation)란 '더 이상 식별가능하지 않도록 하는 조치'를 의미하는 것으로 해석되는 점, '가명화'(Pseudonymisation)란 "추가적인 정보를 이용하지 않고는 특정인을 식별할 수 없도록 하는 조치(그 추가 정보에 대해서는 기술적, 조직적 안전수단에 의해 분리 보관된다는 조건)"를 의미하는 것(제4조 제5호[16])이라고 규정하여, '익명화 처리'(Anonymisation)와 '가명화처리'(Pseudonymisation)를 서로 구분하고 있는 점, '제29조 작업반(Article 29 Data Protection Working Party)'[17]은 암호화 처리 등을 한 가명화 정보는 익명정보가 아니고 여전히 법의 규율을 받는 개인정보라는 해석 기준을 제시하였다는 점[18] 등이 위와 같은 해석을 뒷받침합니다.

이런 점에서 유럽의 여러 국가로부터 우리나라와 동일한 의료정보를 동일한 방식으로 수집하고 있는데 우리나라만 유별나게 형사처벌의 잣대를 들이대고 있다는 한국IMS의 주장은 거짓임을 알 수 있습니다. 한국IMS가 유럽의 여러 국가로부터 개인의 건강정보를 수집하고 있다면, EU의 위 지침에 비추어 그것은 위 지침(Directive)에 따라 익명화 처리(Anonymisation)가 완료된 정보일 것이 틀림없습니다.

다. 소결

위와 같은 점에 비추어, 우리 개인정보보호법이 빅데이터 산업의 발전에 지

---

15) "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

16) Article 4
Definitions
(5)'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

17) EU 개인정보보호지침 제29조에 의해 설치되어 개인정보보호지침의 해석 기준을 제시할 권한이 있는 EU 산하 기관.

18) Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Technique, 2014, 20쪽. "Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation."

장을 주고 있다는 지적은 타당하지 않으며, 특히 본 사안에 대해 유죄 판결이 선고될 경우 우리나라의 빅데이터 산업 발전에 저해가 될 것이라는 주장은 전혀 근거가 없는 것입니다.

또한 법 제18조 제2항 제4호에 규정된 "통계작성 목적으로 특정 개인을 알아볼 수 없는 형태"란 '식별이 가능한지 않은 형태'의 의미로 해석되는데, 약학정보원과 지누스가 한국IMS에 제공한 환자의 처방/조제 정보는 여러가지 방법으로 쉽게 개인을 식별할 수 있는 상태로 제공된 것임이 분명하다는 점에서, 개인정보보호법 위반이 아니라는 피고인들의 변명은 기각되어야 하는 것입니다.

나아가 피고인들은 주민등록번호를 암호화하면 해당 데이터베이스에서 특정 개인을 '식별'할 수는 없다고 주장하고 있는 것으로 보이므로, 이 점에 관하여 나아가 살펴봅니다.

4. 개인정보의 식별성에 관한 논란 - 주민등록번호의 암호화가 식별성을 제거하는 조치인가

가. '개인정보' 개념과 식별가능성의 의미

개인정보보호법은 개인정보의 개념에 관하여 '식별가능한(identifiable)'을 핵심 개념으로 하고 있고, 이는 세계 공통의 것입니다.

개인정보보호법제에 관한 가장 기본적인 법체계인 EU의 개인정보보호지침은 개인정보에 관하여 식별가능한(identifiable) 개인에 관한 정보이라고 규정하고 있고, 피고인들이 많이 인용했을 것으로 보이는 미국의 Health Insurance Portability and Accountability Act(이하 'HIPPA')도 보호대상인 개인의 건강보험정보를 'individually identifiable health information'[SEC. 1171 (6)]으로 정의하고 있습니다.

그럼에도 불구하고 우리의 개인정보보호법이 개인정보의 개념을 넓게 규정하고 있다는 주장이 일부 있고, 본 사안에서도 피고인들은 암호화된 주민등록번호에 의해 건강정보를 '구분'할 수 있을 뿐 특정인을 '식별'할 수 없다고 주장하고 있다고 하나, 이러한 주장은 '개인의 식별가능성'이란 '특정한 시간

과 장소를 전제로 한 해석의 개념'임을 이해하지 못하였기 때문에 발생하는 오해입니다.

'무기명 교통카드'나 외국에서 널리 허용되고 있는 '무기명 선불폰'을 생각하면 쉽습니다. 교통카드도 식별번호(1040 0040 …)가 부여되어 있어, 다른 교통카드와 '구분'할 수 있기는 하나, 그 사용자를 식별할 수는 없습니다(해당 소지자의 소지품을 검사하여 그 번호의 사용자를 확인할 수는 있겠으나, 이를 '식별'이라고 하지는 않습니다.) 대부분의 외국에서는 구입 가능한 선불폰도 마찬가지입니다. 선불폰은 통화가능한 휴대전화 번호가 부여되어 있어 과금은 가능하나, 이 번호 사용자가 누구인지 식별할 수는 없습니다.

그런데 우리나라에서 휴대폰 번호가 외국의 선불폰 번호와 달리 식별가능한 번호가 되는 이유는 기본식별정보와 결합되어 있기 때문이지 그 번호에 원래 식별성이 있기 때문은 아닙니다. 마찬가지로 교통카드의 식별번호가 개인식별 용도로 이용되지 않는 이유는 기본식별정보와 결합되어 있지 않기 때문이지, 원래 식별성이 없기 때문은 아닙니다.

즉, 우리나라의 경우 휴대폰 실명제, 이동통신사를 본인확인기관으로 지정한 제도적 장치 때문에, 휴대폰 번호가 강력한 개인식별번호가 되어 있는 것이며, 개인식별을 회피하면서 다른 정보와 구분하기만 하려면, 다른 식별 정보와 결합가능성이 거의 없어야 합니다.

이런 점에서, 그동안 전문가들이 무분별하게 비판했던 휴대폰 번호 뒷 4자리를 식별가능한 개인정보라고 한 판결(대전지방법원 논산지원 2013고단17 판결)에는 타당한 근거가 있는 것입니다. 개인정보의 식별가능성은 법규정의 문제("다른 정보와 쉽게 결합하여" 문구의 문제)가 아니라, 일정한 상황에서 특정 정보에 의해 특정인을 식별할 수 있는지의 '해석' 문제인데, 휴대폰 번호가 개인식별번호로 기능하고 있는 현실을 전제로 하면(휴대번호 뒷 4자리만으로 1차적인 본인확인을 하는 서비스도 많습니다.), 휴대번호 뒷 4자리만으로도 특정인을 '식별할 수 있다'는 해석은 충분히 가능하기 때문입니다.

역시 전문가들의 많은 비판을 받았던 국제단말기 인증번호(IMEI)를 개인정보로 인정한 판결(서울중앙지방법원 2011. 2. 23. 선고 2010고단5443 판결)도 같은 논리로 당연한 판결인 것입니다. 즉, 기본식별정보와 결합되어 있지 않은

IMEI는 교통카드 번호나 선불폰의 전화번호와 마찬가지로 식별기능은 없습니다. 하지만, IMEI가 이통사 데이터베이스에 휴대번호와 매칭되어 있고, 그 휴대번호가 개인식별번호로 이용되고 있는 우리의 현실을 전제로 하면, 선불폰 제도를 두고 있는 다른 나라에서 IMEI의 의미와 우리나라에서 IMEI의 의미는 서로 다르게 해석할 수밖에 없는 것입니다.

본 사안도 마찬가지입니다.

피고인들도 인정하고 있듯이, 본 사안에서 거래 대상이었던 건강정보 데이터베이스를 의미있게 이용하기 위해서는 적어도 A에 관한 건강정보와 B에 관한 건강정보를 '구분'할 수 있어야 하며, 이렇게 데이터베이스에서 A에 관한 건강정보와 B에 대한 건강정보를 '구분'할 수 있는 기준을 '식별자'나 '키값' 또는 '식별키'(이하 '식별키'라고만 합니다)라 합니다.

한국IMS는 '식별키'를 이용하여 약학정보원으로부터 제공받은 데이터베이스(A 데이터베이스)와 지누스로부터 제공받은 데이터베이스(B 데이터베이스)에서 '식별키'를 이용하여 A 데이터베이스의 甲과 B 데이터베이스의 甲을 동일인으로 식별할 수 있고, 두 데이터베이스를 '식별키'를 기준으로 통합할 수도 있습니다.

그런데 한국IMS는 위 두 단체로부터 넘겨받은 데이터베이스의 '식별키'로 '암호화된 주민번호' 또는 '암호화된 이름+생년월일'을 사용했다고 하면서, 이렇게 암호화된 '식별키'는 권한없는 제3자가 파악할 수 없으므로, 해당 정보에 식별성이 없다고 주장하는 듯하나, 이 주장은 전혀 타당하지 않습니다. '암호화된 주민번호' 또는 '암호화된 이름+생년월일'도 'QA5FRD4'의 형식으로 되어있는, 즉 숫자와 문자가 결합된 '또다른 형식의 식별키'에 불과하기 때문입니다. (문자와 숫자가 128자리로 길게 작성되어 있어도 그 성격이 변하는 것은 아닙니다.)

예를 들면, 앞에서 본 '제29조 작업반'의 '익명화 기술(Opinion 05/2014 on Anonymisation Technique)'이라는 보고서는 '가명화 기술'의 하나로 '건강정보'에 대한 통계처리를 위해 '이름, 주소 및 생년월일'을 해시함수로 처리하는 경우를 예시하고 있습니다(아래 그림 참조).

아래 예시에 의하면, '이름, 주소 및 생년월일'을 해시함수로 처리한 결과값은 'QA5FRD4'와 같은 형식으로 되어 있는 식별키임을 알 수 있습니다. 게다가 보고서의 아래 내용에 의하면, 해시함수로 처리한 가명화 조치는 쉽게 복구될 수 있어, 이를 익명화 조치(즉, 재식별이 안되는 정도의 조치)라 할 수 없다고 지적하고 있기도 합니다.

<Opinion 05/2014 on Anonymisation Techniques 22쪽>

4.3. Shortcomings of Pseudonymisation

- *Health care*

1. Name, address date of birth	2. Period of Special Assistance Benefit.	3. Body mass index	6. Research cohort reference no.
[redacted]	< 2 years	15	QA5FRD4
[redacted]	> 5 years	14	2B48HFG
[redacted]	< 2 years	16	RC3URPQ
[redacted]	> 5 years	18	SD289K9
[redacted]	< 2 years	20	5E1FL7Q

Table 5. An example of pseudonymisation by hashing (name, address date of birth) which can be easily reversed

A dataset has been created to examine the relationship between a person's weight and the receipt of a special assistance benefit payment. The original dataset included the data subjects' name, address and date of birth but this has been deleted. The research cohort reference number was generated from the deleted data using a hash function. Although the name, address and date of birth were deleted from the table, if a data subject's name, address and date of birth is known in addition to knowing the hash function used it is easy to calculate the research cohort reference numbers.

(위 표 중 까맣게 되어 있는 부분은 제29조 작업반의 홈페이지에 게시되어 있는 원본 자체의 오류이며, 임의의 이름, 주소, 생년월일이 기재되어 있는 듯합니다.)

이에 따라 쟁점은 한국IMS가 'QA5FRD4'와 같은 식별키를 통해 특정인을 '식별할 수 있는지'가 쟁점인 것인지, 개인정보처리자인 피고인들이(특히 한국IMS가) 그 식별키를 이용하여 특정인을 '식별하고자 하는 의도가 있었는지' 여부가 아니며, 'QA5FRD4'의 형식으로 된 암호화된 주민번호도 또다른 '식별키'인 이상 아래에서 자세히 살펴보는 바와 같이 그 '식별키'로 특정인을 식별해 내는 것은 당연히 가능합니다.

나. 개인정보의 암호화는 식별성을 제거하는 조치인가

우리 개인정보보호법 상 암호화는 보안수단이지 개인정보보호법 제18조 제1항 제4호의 '특정 개인을 알아볼 수 없는 형태'에 관한 것이 아닙니다.

법 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다."고 규정하고 있고, 법 시행령 제30조 제1항은 다른 안전성 확보 조치와 함께 "개인정보를 안전하게 저장·전송할 수 있는 암호화기술의 적용 또는 이에 상응하는 조치"를 규정하고 있습니다. 또한, 법 제23조 제1항은 "제29조에 따른 안전성 확보 조치", 법 제24조 제3항은 "암호화 등 안전성 확보에 필요한 조치"라고 규정하고 있고, 위와 같은 법령 규정을 구체적으로 규정하기 위한 '개인정보의 안전성 확보조치 기준'(행정자치부 고시)은 제7조에서 '개인정보의 암호화'라는 제목으로 '안전한 암호알고리즘으로 암호화'해야 하는 대상과 기준을 규정하고 있는 점에 비추어, 우리 개인정보보호법 상 개인정보의 암호화는 식별가능성을 제거하는 조치가 아니라 분실이나 유출, 위변조로부터 개인정보의 안전을 보호하기 위한 수단에 불과합니다.

앞에서 살펴보았듯이, EU의 개인정보보호지침(Data Protection Directive)이나 일반개인정보보호규정(GDPR)도 암호화 조치를 그 결과가 여전히 개인정보에 해당하는 '가명화(Pseudonymisation) 조치'의 하나로 제시하고 있을 뿐입니다.

또한 '제29조 작업반'은 암호화, '해시 함수 적용', '토큰화(보안기술의 일종)'를 '가명화 기술'의 일부로 제시하며, '가명화'란 익명화 수단이 아니고, 단지 정보주체의 원래 식별정보가 포함된 데이터베이스와 연결성을 감소시키는 안전 수단으로, 개인정보보호기준이 그대로 적용된다는 해석기준을 제시한 바 있습니다[19].

다만, GDPR은 개인정보관리자가 가명화 기술을 이용하여 개인정보를 가명화할 경우 목적 외 이용(further processing)의 범위를 넓게 인정하는 등의 혜택을 부여하여(GDPR 제6조 제4항) 가명화 조치를 유도하고 있을 뿐입니다.

---

19) Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Technique 20면

따라서 위와 같은 개인정보보호의 기준에 의할 때, 주민등록번호 또는 '이름+생년월일'의 식별정보를 암호화한다고 하더라도 그 식별성이 감소할 수는 있으나 식별가능성이 없다고 할 수 없으므로, 여전히 개인정보의 보호기준이 적용되는 개인정보라는 그 성격이 변하는 것은 아닙니다.

한편, 피고인들은 주민등록번호나 '이름+생년월일'을 '일방향 암호화 방식'으로 보안조치를 하였고, 특정 정보를 일방향으로 암호화할 경우 원래의 정보를 복원하는 복호화를 할 수 없으므로, 일방향으로 암호화된 주민등록번호나 '이름+생년월일'을 복원할 수 없어 결국 비식별 정보라고 주장하는 것으로 알려져 있습니다.

하지만, 규칙이 없는 특정 정보를 일방향으로 암호화할 경우 그 보안효과가 높다고 할 수는 있으나, 일정한 규칙으로 조합되어 있는 주민등록번호나 '이름+생년월일'의 일방향 암호화는 그 보안효과가 거의 없습니다. 특히 그 조합방식이 사실상 공개되어 있고 단순하고 명료한 구성으로 되어 있는 주민등록번호의 경우, '일방향 암호화' 수단으로 암호화되어 있다고 하더라도, 원래 정보를 복호화하는 것이 그렇게 어려운 일은 아니며, 실제로 한국IMS가 수집한 암호화된 주민등록번호정보를 기초로 원래의 주민등록번호를 복원하기도 하였으며(아래 기사 참조), 그 내용은 참고자료1로 제시하는 바와 같이 논문으로 발표되기도 하였습니다(참고자료1 번역문 참조).

정부, 개인의료정보 빅데이터 개방하겠다는데…

'암호화된 주민번호' 너무 쉽게 풀렸다

미국 하버드대팀, 이미 지난해에
2만3천명 처방전 암호 100% 해제
"한국 주민번호 생일·성별 담겨
프로그램 몇번 돌리니 쉽게 풀려"

전문가 "민감한 개인정보 노출 위험
본인 동의 없이 공개 말아야"

정부가 개인의 민감한 의료정보를 암호화 등 비식별 조치해 민간에 개방하겠다는 방침을 밝힌 가운데, 미국에서 암호화된 한국 주민등록번호를 100% 해제할 수 있다는 연구결과가 나왔다.

국회 보건복지위원회 소속 정춘숙 의원(더불어민주당)이 25일 번역해 공개한 미국 하버드대학교 라타냐 스위니 교수 연구팀의 2015년 논문 '처방전 데이터상 공유되는 대한민국 주민등록번호의 익명성 해제'를 보면, 연구팀은 한국인 사망자 2만3163명의 처방전 데이터의 암호화된 주민등록번호를 전부 해제하는 데 성공한 것으로 나타났다.

연구팀은 암호화된 주민등록번호를 논리적 추론 방식과 자동탐색실험, 두 가지 방식으로 모두 해제했다. 논리적 추론 방식은 각각의 자리에서 발견되는 문자의 빈도를 통해 어떤 자리의 어떤 수가 어느 문자로 치환됐는지를 추론하는 방식인데, 논문은 한국의 주민등록번호는 임의번호가 아닌 생년월일과 성별 등 인구통계학적 개인정보를 담고 있기 때문에 더 쉽게 풀 수 있었다고 밝혔다.

이에 따라 정부의 개인정보 비식별화 가이드라인을 재검토해야 한다는 목소리가 높아질 것으로 보인다. 행정자치부는 개인정보를 비식별화(암호화)하면 이를 개인정보로 보지 않아 동의 없이도 처리할 수 있다는 가이드라인을 내놨고, 보건복지부는 이를 근거로 지난달 30일 건강보험심사평가원과 국민건강보험공단이 보유한 진료내역 등 5조 1027억건의 의료데이터를 민간에 개방해 빅데이터 산업에 활용토록 하겠다고 발표했다. 복지부는 주민등록번호 등은 가리거나 암호화해 문제없다는 입장이지만, 빅데이터의 속성상 작은 조각들이 연결돼 식별 가능한 개인정보로 변하는 것은 시간문제라는 것이 전문가들의 지적이다.

강장묵 고려대 컴퓨터학과 교수는 "연구에서도 보이듯 비식별화된 정보는 언제든 재식별의 위험성이 있다. 특히 우리나라처럼 이미 수많은 개인정보가 유출돼 거래되고 있는 상황에서는 흩어져있는 데이터들이 연결돼 민감한 개인정보가 그대로 노출될 위험이 높다"고 지적했다. 정춘숙 의원은 "비식별화의 문제가 확인된 이상 진료기록 등 민감정보는 어떠한 경우에도 본인 동의 없이 공개해서는 안 된다"고 지적했다.

이번 논문은 또 "한국이 주민등록번호를 임의번호 체계로 개편하는 데 3조1000억~4조원의 비용이 들 것이라 추정하지만, 만약 개편하지 않는다면 이 제도와 이 제도를 사용하는 사람들에게 경제적 위험을 줄 것"이라고 지적하기도 했다. 현재 주민등록번호 체계를 임의번호로 전면 개편하도록 하는 주민등록법 개정안이 국회에 발의돼 있다.

최승 기자 ceason@hani.co.kr

설사 일방향 암호화 수단이 워낙 강력하여 암호화된 주민등록번호에서 원래의 주민등록번호를 복원할 수 없다고 하더라, 한국IMS가 구매한 건강정보 데이터베이스에서 특정인을 식별하는 것이 어려운 일인 것도 아닙니다. 그 방법은 이렇습니다. 암호화에 사용된 해시 함수와 특정한 주민등록번호를 알고 있는 사람은 '식별키'인 암호화된 주민등록번호('QA5FRD4'의 형식으로 되어 있는 것)를 해당 데이터베이스에서 찾은 후, 그 식별키로 특정인을 식별할 수 있기 때문입니다. 예를 들면, 甲의 주민등록번호를 알고 있거나, 또는 오늘(2016. 12. 7.) 서울에서 태어난 남자아이에게 161207-30xxxxx와 같은 형식으로 주민번호가 부여될 것임을 유추할 수 있는 사람은 161207-30xxxxx의 번호를 해당 해시 함수로 일방향으로 암호화하여 'QA5FRD4'와 같은 형식으로 된 문자+숫자 조합의 식별키를 얻을 수 있고, 이 식별키로 건강정보 데이터베이스를 검색하면 해당 데이터베이스에서 甲을 찾을 수 있게 되므로, 건강정보 데이터베이스에서 甲을 찾기 위해 굳이 일방향으로 암호화된 주민등록번호를 복원할 필요는 없는 것입니다.

따라서 주민등록번호나 '이름+생년월일'을 일방향 해시 함수로 암호화하였다는 이유로 해당 정보의 식별성이 없다는 피고인들의 주장은 전혀 타당하지 않은 것입니다.

5. 결론

이상에서 살펴본 바와 같이, 우리 개인정보보호법은 빅데이터의 처리에 관하여 EU의 개인정보보호규정과 유사한 내용의 규정을 두고 있으므로 우리 개인정보보호법이 빅데이터 산업의 발전에 장애가 되고 있다는 주장은 타당하지 않으며, 본 사안의 경우 더더욱 빅데이터 산업의 발전과 관계가 없는데다, 개인정보의 암호화는 개인정보의 식별성을 제거하는 수단이 아닌 개인정보의 안전성을 확보하는 수단에 불과하고, 특히 주민등록번호나 '이름+생년월일'의 일방향 해시 함수를 이용한 암호화는 식별가능성을 제거하는 조치라 할 수도 없다는 점에서 피고인들의 주장은 잘못된 것이라는 점을 분명히 지적하는 바입니다.

참고자료

1. Latanya Sweeney, Ji Su Yoo, “처방 데이터상 공유되는 대한민국 주민등록번호의 익명성 해제” 번역문(국회도서관 번역)
2. 이은우, “마케팅 활용 목적 빅데이터 활용과 판매: 개인정보 플랫폼 기업의 탐욕과 비식별화 조치 가이드라인”, 2016. 9. 7., 빅데이터 시대 개인정보 보호를 위한 정책토론회 자료집
3. “암호화된 주민번호’ 너무 쉽게 풀렸다”, 한겨레신문 2016. 9. 25.

2016년 12월 9일

제출자

1. 진보네트워크센터
서울특별시 서대문구 독립문로8길 23 3층
대표자 이종회 (인)

2. 경실련 시민권익센터
서울특별시 종로구 동숭동 50-2
대표자 황이남 (인)

3. 건강권실현을 위한 보건의료단체연합
(건강사회를위한약사회 건강사회를위한치과의사회 노동건강연대 인도주의실천의사협의회 참의료실현청년한의사회)
서울특별시 종로구 이화동 26 - 1 3층
대표자 김정범 (인)

서울중앙지방법원 제22형사부 귀중