

판례평석

처방정보의 비식별화를 통한 제3자 제공과 관련한 형사 판결 검토

- 서울중앙지법 2020. 2. 14. 선고 2015고합665 판결에 대한 검토 -
Commentary on Criminal Decision with regard to Data Transfer of
the De-identified Medical Information

박 규 홍(Kyuhong Park)*

목차

- I. 들어가며
- II. 이 사건의 개관 및 공소사실의 요지
- III. 공소사실의 요지 및 법원 판단의 요지
- IV. 이 사건의 시사점
- V. 결론

I. 들어가며

우리 사회는 지난 2016년 알파고라는 AI 기술을 기반으로 개발된 바둑 프로그램에 의하여 빅데이터를 기반으로 하는 4차 산업혁명이 이미 우리 곁에 다가와 있음을 알게 되었다. 당시의 알파고는 역사상 수많은 바둑기사들이 남긴 ‘기보’를 학습하여 고금 최강의 바둑기사(?)가 되었다.

바둑과는 무관하지만 이미 축적된 수많은 데이터(또는 기록)를 기반으로 또다른 알파고가 등장할 수 있는 분야가 있다. 바로 의료분야이다. 의료데이터의 분석과 활용은 의료서비스의 품질개선,

개인별 질병진단 및 치료서비스 향상 등 의료 시스템 전반에 걸쳐 혁신을 유도할 수 있을 것으로 예측¹⁾되고 있다.

과거의 데이터가 모두 공개되어 활용이 쉬웠던 바둑 분야와 달리, 의료정보는 개인의 사생활 침해의 가능성이 매우 높은 민감한 정보들로 구성되어 있으며, 이로 인하여 높은 기대수요에도 불구하고 데이터의 활용이 어렵다. 의료정보의 활용을 위해서는 안전한 활용기술, 의료정보를 둘러싼 이해관계자 사이의 갈등조정 - 예컨대, 데이터 생산자인 의사와 데이터를 집적·보유하게 되는 자 사이의 이해관계, 정보주체인 환자들의 사생활 침해우려 해소 - 등과 같은 여러 문제가 해결되어야 한다. 미국, 프랑스 등 해외 각국에서는 의료정보의 활용을 위하여, 개인정보 보호에 대한 상황을 인식하고 연구 목적 등의 2차 활용을 위한 비식별 기술을 연구하고 그와 관련한 가이드를 제시하고 있다.²⁾

의약분업 체계와 국민건강보험제도가 확립된 우리나라에서는 의료기관인 병·의원은 환자를 진료하고, 환자의 치료 등을 위하여 적절한 약을 처방

* 법무법인(유한) 세종 변호사(Shin & Kim LLC. Partner), 공학석사 (통신방송공학)

1) 김재한, 의료데이터 활용을 위한 개인정보 비식별화 기술 및 프로그램 동향, 2018. 8., 보건산업브리프 Vol. 268
2) 김재한, 앞의 논문

한다. 이러한 의사의 처방은, 환자에 의하여 약국에 정확하게 전달되어 약이 지급된다. 이러한 과정을 거쳐 의사가 작성하는 ‘처방정보’는 약국이 사용하는 약국관리시스템 등에 ‘조제정보’로 전달된다. 이 사건은 약국관리시스템에 입력된 조제정보를 수집하여, 비식별화 조치를 거쳐 제3자에게 제공된 행위가 문제된 사안이다. 아래에서는 의료데이터를 활용한 사업에 있어 이 사건의 시사점이 무엇인지 살펴보고자 한다.

II. 이 사건의 개관 및 공소사실의 요지

1. 이 사건의 개요 및 조제정보의 제3자 제공

A재단은 약국관리 프로그램인 팜매니저2000(이하 ‘PM2000’)을 운영하는 주체로서 의약품 관련 정보의 수집 및 데이터베이스 구축, 의약품정보 관련 연구 용역사업 수행 등을 목적으로 하는 재단 법인이다.

의사가 환자에게 발행하는 처방전에는, 환자의 성명 및 주민등록번호, 의료기관의 명칭 및 전화번호, 질병분류기호, 의료인의 성명, 면허종류 및 면허번호, 처방의약품의 명칭, 분량 및 용법, 처방전 발급 연월일 및 사용기간 등이 기재되어 있다. 환자가 처방전을 약국에 제출하면 각 약국은 해당 약을 조제하여 환자에게 지급하고, 위 정보를 PM2000 프로그램에 입력하여 그 정보를 토대로 건강심사평가원에 조제료, 복약지도료 등을 청구하게 된다.

A재단은 2010. 12. 30. B사와 조제정보의 공동사용에 대한 약정을 체결하였다. A재단은 2011. 1. 28.경 각 약국에 저장된 처방전 관련 정보를 A재단으로 자동 전송하는 기능을 추가한 PM2000 프로그램 업데이트를 실시하여, PM2000 프로그램을 통해 입력된 조제정보 중 일부를 암호화하여 각 약국의 서버 외에 A재단의 중앙서버에도 저장

되도록 하였다.

이후 A재단은 PM2000 프로그램을 통하여 수집한 일부 암호화된 조제정보를 B사에 제공하였다.

2. 조제정보의 수집 및 그 일부에 대한 암호화

가. 사업 개시 후 개인정보보호법의 시행

B사가 A재단으로부터 조제정보를 제공받던 중인 2011. 3. 29. 개인정보보호법이 제정되어 같은 해 9. 30.부터 시행되었다. 아울러 주민등록번호에 대한 원칙적인 처리금지 규정인 개인정보보호법 제24조의2가 2013. 8. 6. 신설되어 1년 후인 2014. 8. 6.부터 시행되었다.

나. A재단과 B사가 처리한 정보

A재단이 약국으로부터 전송받아 집적한 정보 중 개인에 대한 식별가능성이 있는 정보는 아래와 같이 의사의 성명, 면허번호와 환자의 주민등록번호이다. 해당 정보가 제거되고 남은 정보는 직접적으로 처방에 관한 정보 뿐이어서 특정 개인을 식별할 수 있는 정보로 보기는 어렵다.

1) 의사의 성명 및 면허번호

A재단의 B사에 대한 최초 정보제공시인 2011. 1. 말경부터 2012. 2. 2.까지는 의사의 실제 성명과 면허번호로, 그 다음날부터는 암호화되어 B사에 각 제공되었다. 이에 대하여는 복호화 함수가 존재하지 않았다.

2) 환자의 주민등록번호

가) 1기 암호화

A재단의 B사에 대한 최초 정보제공시인 2011. 1. 말경부터 2014. 6.경까지는 13자리의 주민등록번호 중 홀수 자리와 짝수 자리를 각 다른 암호화 규칙에 따라 영어 알파벳으로 치환한 다음 양끝 2 자리에 임의의 알파벳으로 잡음(노이즈, noise)을 추가하는 방식의 양방향 암호화가 이루어졌다.

나) 2기 암호화

A재단은 1기 암호화의 방식이 부실하다는 안전 행정부의 행정지도에 따라 2014. 6.경부터 2014. 9.경까지는 복호화가 불가능한 일방향 암호화 방식인 SHA-512³⁾ 방식으로 환자의 주민등록번호가 암호화되었다

다) 3기 암호화

A재단은 주민등록번호의 처리가 원칙적으로 금지된 2014. 10.경 이후부터 B사에 대한 정보제공이 종료된 2015. 1.경까지는 주민등록번호가 아니라 성명, 생년월일, 성별로 환자를 특정한 후 이를 2기 암호화와 동일한 일방향 암호화 알고리즘인 SHA-512 방식으로 암호화하여 제공하였다

Ⅲ. 공소사실의 요지 및 법원 판단의 요지

1. 공소사실의 요지

검사는 2015. 7. 23. 피고 A재단 및 A재단의 대표자 및 직원, B사의 대표자 및 직원에 대하여 개인정보보호법상 민감정보에 해당하는 환자의 조제정보 등을 처리하거나 무단으로 제공하였다는 개인정보보호법위반 등의 공소사실로 기소하였다.

2. 법원 판단의 요지

법원은 A재단과 B사 사이의 정보제공행위에 대하여, 재식별가능성이 인정되어 개인정보를 처리한

행위로 판단하였다.

그러나, A재단이 B사에 제공하려던 정보에 대하여 꾸준히 암호화를 한 사정을 비롯하여 A재단과 B사 사이에 진행된 데이터 처리의 제반사정을 종합적으로 고려하여, 개인정보를 처리한다는 고의가 인정되지 않는다는 이유로 모두 무죄로 판단하였다.⁴⁾

Ⅳ. 이 사건의 시사점

1. 객관적 구성요건 : 비식별화의 적정성 평가기준

가. 선행 민사사건의 개인정보 여부 판단기준

이 사건과 동일한 사실관계에 대하여 이미 민사사건에 대한 1, 2심 법원의 판결이 선행하였는바, 민사사건에서 제시한 개인정보 해당 여부에 대한 판단기준을 먼저 살펴보고, 이 사건 법원의 판단을 살펴보도록 한다.

1) 민사 1심 법원이 제시한 판단기준

민사 1심 법원은, “개인정보는 해당 정보를 처리하는 자의 입장에서 특정 개인을 식별할 수 있는 (identifiable) 정보이므로, 개인정보에 암호화 등 적절한 비식별화(de-identification) 조치를 취함으로써 특정 개인을 식별할 수 없는 상태에 이르면 이는 식별성을 요건으로 하는 개인정보에 해당한다고 볼 수 없고, 따라서 정보주체의 동의 없이 통계작성 등의 용도로 이용되거나 제3자에게 제공되더라도 개인정보 보호법을 위반한 것이라고 볼 수 없다”고 하면서, “다만, 비식별화 조치가 이루어졌다고 하더라도 재식별 가능성이 현저하다면 적절한 비식별화 조치가 이루어지지 않은 것이므로 여전히 개인 정보 보호법이 적용되는 개인정보에 해당한다고 할 것이고 적절한 비식별화 조치가 이루어진 것인지 여부는 원본 데이터의 특성, 비식별화

3) SHA 계열의 해시함수는 1993년 미국 표준 기술 연구소(NIST)에 의해 처음으로 발표되었으며, 최초 발표된 함수를 SHA-0라고 부른다. 그 이후 해시 길이를 늘린 SHA-1, SHA-128, SHA-256, SHA-384, SHA-512 등의 알고리즘이 발표되어 왔다. 암호 알고리즘은 현재 시점에서 안전한 알고리즘이라 할지라도 몇 년 후에는 쉽게 해독이 되어 안전하지 않게 될 수 있다. 컴퓨팅 능력은 나날이 발전하고 새로운 분석 기법도 계속 개발되고 있기 때문이다. 따라서 암호 알고리즘은 그때그때의 state-of-the-art에 의해 재평가되어야 한다(박영호, 공개키 암호, 2007). 우리나라는 한국인터넷진흥원에서 인터넷 홈페이지를 통하여 암호알고리즘의 안전성을 평가하여 그 결과를 공개하고 있다.

4) 이 사건에서 A재단과 B사 이외에 정보처리프로그램을 개발·공급한 C사가 있었고, C사에 대하여 벌금형이 선고되었으나, 주요쟁점과 거리가 있으므로 본고에서는 별도로 다루지 아니한다.

된 정보가 사용된 특정한 맥락이나 상황, 비식별화 조치에 활용된 기법·세부기술의 수준, 비식별화된 정보를 제공받은 자의 이용목적 및 방법, 이용기간, 전문지식이나 기술력·경제력에 따른 재식별화 능력, 비식별화된 정보를 제공받은 자가 재식별화로 얻을 수 있는 이익의 유무, 비식별화된 정보를 제공받은 자의 개인정보 보호 수준, 비식별화된 정보와 외부 정보 사이의 결합 가능성, 비식별화된 정보를 제공한 자와 제공받은 자의 관계, 비식별화된 정보에 대한 접근권한 관리 및 접근통제 등을 종합적으로 고려하여 판단해야 할 것"이라고 판시하였다.

2) 민사 2심 법원이 제시한 판단기준

민사 2심 법원은, 1심 법원의 원칙론을 그대로 인정하면서도, "다만, 비식별화 조치가 이루어졌다고 하더라도 재식별 가능성이 합리적으로 존재한다면 적절한 비식별화 조치가 이루어지지 않은 것이므로 여전히 개인정보에 해당한다"고 판시하였다.

나. 이 사건 법원의 판단기준

이 사건 법원은 "개인정보에 암호화 등 적절한 비식별화 조치를 취함으로써 특정 개인을 식별할 수 없는 상태에 이른다면 개인정보에 해당하지 않으나, 비식별화, 암호화 조치가 이뤄졌더라도 재식별 가능성 또는 복호화 가능성이 합리적으로 존재한다면 여전히 개인정보에 해당한다고 보아야 한다"고 판시하여, 민사 2심 법원의 판단기준과 동일한 기준을 제시한 것으로 보인다.

다. 검토 : 재식별 가능성 판단요건에서 현저성은 제외함이 타당

1) 판단기준에 대한 검토

민사 1심 법원은 재식별 가능성에 대한 "현저성"을 추가적 요건으로 제시하면서, 비록 재식별 가능성이 있더라도 제반 사정을 고려하여 그 가능성이 현저한 수준에 이르지 않으면 재식별 가능성을 부정하는 입장을 취하였다.

반면, 민사 2심 법원은 이러한 "현저성"을 요건으로 보지 아니하면서, 재식별 가능성이 합리적으로 존재하는 것만으로 비식별화 조치가 이루어지지 않은 것으로 보아 개인정보에 해당한다고 판단하여야 한다고 보았다.

재식별 가능성이란, 유무(有無) 또는 존부(存否)의 문제이지, 그 정도의 차이에 따라 판단결과가 달라질 문제는 아닌 것으로 생각된다. 즉, 어느 개인정보처리자의 입장에서 합리적으로 재식별 가능성이 있다면, 그 가능성이 현저한지 여부와 무관하게 재식별 가능성을 인정함이 타당하고, 재식별 가능성이 있는 한 개인정보를 처리하고 있는 것으로 봄이 상당하다.

2) 환자 주민등록번호의 개인정보 해당 여부

1기 암호화된 정보는 B사의 임원이 암호화 여부 및 방법에 관하여 논의하였던 점, 암호화 방법이 매우 간단하여 수사기관에서도 쉽게 복호화하였던 점 등을 고려하여, 재식별 가능성을 인정하였다.

한편, 2기 암호화 방식과 3기 암호화 방식에 대하여, A재단은 B사에 ① 2기 암호화 방식의 주민등록번호와 이에 대응되는 1기 암호화 방식의 주민등록번호를 기재한 매칭 테이블을, ② 3기 암호화 방식으로 생성된 환자의 고유번호와 이에 대응되는 2기 암호화 방식의 주민등록번호를 기재한 매칭 테이블을, 각각 외부저장매체에 저장하여 제공하였다. 이러한 점에 비추어 볼 때, 2, 3기 암호화 방식도 1기 암호화 방식과 결합하여 개인을 식별할 수 있다고 봄이 타당하므로, 이 사건 정보는 1기 암호화 방식으로 암호화된 것뿐만 아니라 2, 3기 암호화 방식으로 암호화된 것까지 모두 개인정보에 해당한다고 보았다.

2. 주관적 구성요건 : 개인정보 처리에 대한 '고의'

가. 이 사건 법원의 판단기준

법원은 "정보가 식별가능한 개인정보에 해당한

다는 것과 행위자가 그 정보를 식별가능한 개인정보로 인식했는지 여부는 별개의 문제”라고 판시하면서, “특히 개인정보가 비식별화 조치 또는 암호화 조치가 된 경우, 그와 같은 정보를 처리하는 자에게 고의가 있었다고 보려면, 이를 식별화 또는 복호화해 처리할 수 있다는 인식과 함께 그와 같은 정보를 식별가능한 형태의 정보를 치환해 처리하는 것을 용인하는 의사까지 인정되어야 한다”고 보았다.

나. 구성요건적 고의의 인정요건

객관적으로 개인정보에 해당하는 경우라 하더라도, 범죄가 성립하여 형사처벌을 받기 위해서는 구성요건해당성이 인정되어야 한다. 법원은 A재단과 B사가 정보를 제공하는 과정에서 굳이 암호화 알고리즘을 적용하는 행위를 하였던 점에 착안하여, 과연 해당 업무를 수행한 관련자들에게 개인정보를 처리한다는 사실에 대한 고의가 인정될 수 있는지 여부를 살펴본 것이다.

대법원은 일관하여 ‘고의’의 인정기준에 대하여, “미필적 고의가 있었다고 하려면 범죄사실의 발생 가능성에 대한 인식이 있음은 물론, 나아가 범죄사실이 발생할 위험을 용인하는 내심의 의사가 있어야 하며, 그 행위자가 범죄사실이 발생할 가능성을 용인하고 있었는지의 여부는 행위자의 진술에 의존하지 아니하고, 외부에 나타난 행위의 형태와 행위의 상황 등 구체적인 사정을 기초로 하여 일반인이 라면 당해 범죄사실이 발생할 가능성을 어떻게 평가할 것인가를 고려하면서 행위자의 입장에서 그 심리상태를 추인하여야 한다”고 판시하여 왔는바(대법원 2009. 2. 26. 선고 2007도1214 판결 등), 이 사건 법원은 대법원의 판례를 그대로 따른 것으로 타당한 기준으로 생각된다.

다. 이 사건의 경우 : 개인정보 처리의 고의 부정

이 사건 법원은 A재단과 B사 사이의 계약 내용, 정보제공의 목적, B사의 정보활용방식 등 제반 사정을 종합적으로 고려하여, 관련자들에게 개인정보

를 처리한다는 인식과 재식별하려는 의사가 인정된다고 보기는 어렵다고 보았다.

또한 “A재단은 암호화된 상태로 수집된 주민등록번호를 그대로 B사에 제공하기만 하면 될 뿐이고 굳이 암호화된 상태의 주민등록번호를 실제 주민등록번호로 복호화할 아무런 이유나 동기가 없었다는 점, 아울러 A재단이 B사와 데이터공급계약을 체결하고 약국으로부터 PM2000 프로그램을 통해 환자의 주민등록번호가 포함된 조제정보를 수집한 시점은 개인정보보호법이 시행된 2011년 9월 30일 이전인바, 개인정보보호법에서 금지하는 행위에 해당할 수 있다는 사정까지 예견하고 주민등록번호를 암호화하였던 것으로 볼 수 없어, 암호화된 주민등록번호를 복호화할 의사가 있었다고 단정하기 어렵다고 보았다.

결국 법원은 이러한 사정들을 고려하여, A재단과 B사의 개인정보 처리행위에 대한 고의를 부정하였다.

3. 소결 : 개인정보처리의 고의 요구의 의미

이 사건 법원의 판단에 비추어, 향후로는 개인정보의 비식별화가 쟁점이 되는 사건이 발생하더라도 민사사건 외에 형사사건화가 되기는 어려워진 것으로 생각된다. 비식별조치의 적정성이나 재식별 가능성 등은 사업자의 역량이나 기술적 수준에 따라 사후적으로 부족하였던 것으로 판단될 여지가 있을 것이지만, 비식별 조치를 취한 사업자에게 개인정보를 처리하려는 고의가 인정되기는 어려울 것이기 때문이다.

이 사건은 데이터 산업의 발전 과정에서 이해관계자 사이의 갈등이 발생하게 되더라도, 사업자 간 분쟁이 민사적 수단으로 해결되도록 하고, 형사절차의 진행을 최소화함으로써 불필요한 형사처벌의 위험을 미연에 방지하게 된 데 그 의의가 있다고 생각된다.

V. 결론

우리 곁에 훌쩍 다가온 4차 산업혁명에는 기존 산업 간 경계를 허물고 있다. 정부는 이러한 시대를 대비하기 위하여 규제샌드박스과 같은 규제혁신제도를 마련하고 있다.

비록 이 사건은 개인정보보호법이 도입되기 전에 개시되었던 서비스였으나, 전반적으로 비식별화를 통한 데이터의 활용에 대한 중요 쟁점을 포함하고 있는 사건이다. 특히 2020년 데이터 3법(개인정보보호법, 정보통신망법, 신용정보법)의 개정으로 가명정보가 도입되는 등 개인정보의 활용을 위한 제도적 뒷받침이 시작된 상황에서 이 사건은 향후 참고자료가 될 것으로 기대된다.

개인정보의 문제는 해킹 등 기술적 방법에 의한 정보유출과 같이 범죄사실만 입증되면 위법성이 인정되는데 별다른 어려움이 없었던 시대에서, 새로운 방식으로 정보를 활용하는 사업을 전개하는 과정에서 범위만 요소를 포함하는지 여부가 문제되는

복잡다단한 시대로 이미 진입하였다. 이 사건 피고인들은 2015년 기소가 이루어진 이후 판결이 선고되기까지 6년의 시간이 흐르는 동안 형사처벌의 두려움에 떨어야 했고, 아울러 해당 사업이 제대로 이루어지지 못하는 등의 부작용을 남겼다는 점에서 아쉬움이 남는다.

물론 정보주체의 정당한 권리를 침해하거나, 저해할 우려가 있는 행위는 엄단이 되어야 할 것이다. 혁신서비스가 도입되는 과정에서 반사적인 손실을 입게 되는 기존 이해관계자들과의 원만한 관계설정도 선행되는 것이 필요할 수 있다. 그러나 산업 발전에 도움이 되는 방향의 데이터 활용사업의 등장이 형사절차와 같이 극단적인 방식을 통하여 저해되는 것은 우리 사회 전체의 공리를 후퇴시키는 부적절한 방식이 될 수밖에 없다. 이 사건 판결 이후로는 위법성 논의에 대한 폭넓은 논의를 통한 지속적 서비스 구조의 보완과 같은 점진적인 발전을 도모하는 방식의 갈등해결 구조가 정착되기를 희망한다.