

「개인정보 보호법」상의 ‘개인정보’ 개념에 대한 해석론

- 익명화된 처방전 정보를 중심으로 -

Analyzing the Concept of ‘Personal Data’ under the
Personal Data Protection Act of Korea

- With Special Reference to De-identified
Medical Prescription Data -

이인호(Lee, Inho)*

목 차

- I. 문제의 제기
- II. 개인정보보호법의 존재이유 : ‘보호’와 ‘이용’의 균형
- III. 개인식별성에 관한 주요 외국 입법례의 비교
 - 1. 보호대상이 되는 ‘개인정보’의 필수적 개념요소 : 個人識別性
 - 2. 주요 외국법의 ‘개인정보’ 개념에 대한 비교법적 분석
- IV. 「개인정보 보호법」의 해석론 : 개인식별성의 세 가지 판단방법
- V. 결론

요 약

‘암호화된 주민등록번호를 가진 1966년 8월 30일(생년월일)에 출생한 여자(성별)가 2014년 1월 10일 진해연세병원 정형외과에서 질병기호 S934의 병으로 대응제약의 알비스정을 5일치 처방받았다.’는 내용의 處方箋(처방전) 정보가 있다. 이 匿名化한 환자의 處方箋 정보는 「개인정보 보호법」 제2조 제1호에서 규정하는 ‘개인정보’에 해당하는가? 그리하여 동 법률의 규율대상이 되는가? 이 정보의 주체가 ‘누군가 특정한 개인’이라는 점은 분명하다. 그런데 이 정보가 만일 그 특정한 개인을 알아볼 수 있는

* 중앙대학교 법학전문대학원 교수/헌법·정보법

‘개인정보’에 해당한다면, 이 정보는 ‘건강에 관한 정보’로서 법 제23조의 ‘민감정보’에 해당하게 되고 따라서 정보주체의 사전 동의를 받거나 법령이 처리를 허용하는 경우 외에는 그 처리(수집·이용·제공)에 대해 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해지게 된다(제71조 제3호).

아니면, 이러한 정보는 그 정보주체가 누구인지 알아볼 수 없는 정보이기 때문에 ‘개인정보’에 해당하지 않고, 따라서 그 정보주체의 동의 여하에 관계없이 의약품의 연구나 통계분석 목적을 위해 정보보유자(약국 등)와 통계분석자(데이터마이닝회사) 사이의 제한적인 공유를 통해 이 정보를 활용하는 것이 현행법의 해석론으로 허용될 것인가?

「개인정보 보호법」 제2조 제1호는 “개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.”고 개념정의하고 있다. 이 사안에서의 핵심쟁점은 ‘암호화된 주민등록번호, 생년월일과 성별’을 가지고 그 특정의 누군가를 식별해낼 수 있느냐 하는 것이다. 이 쟁점은 단순히 법 제2조 제1호의 ‘개인정보’ 개념의 해석·적용에 관한 문제이지만, 좀 더 넓은 관점에서 보면, ‘익명화한 처방정보에 대해 연구·통계 목적으로 전문적인 분석을 자유롭게 허용할 것인가’에 관한 문제이다. 물론 익명화의 방식에 있어서 그 식별성이 쉽게 복원될 수 있는 것이라면 문제가 되겠지만, ‘복호화가 불가능한 암호화된 주민등록번호’는 그 식별성의 복원이 불가능하고, 또한 ‘생년월일과 성별’ 정보는 개인식별자(identifier)가 아니어서, 이런 수준의 익명화처리라면 ‘연구·통계 목적’으로 일반 공개가 아닌 제한적인 유통이 허용되어야 할 것으로 생각된다. 이 글은 비교법적 분석을 통해 한국 「개인정보 보호법」 상의 ‘개인정보’의 개념에 대한 해석론을 밝히면서 위 익명화한 처방전 정보가 ‘개인정보’에 해당하지 않는다는 점을 논증한 것이다.

주 제 어

개인정보보호법, 개인정보, 식별가능한 개인정보, 익명화, 비식별화, 개인식별자, 처방전정보

I. 문제의 제기

(1) 아래 <표 1>과 같이 匿名化한 환자의 處方箋 정보는 「개인정보 보호법」(2011. 9. 30. 시행. 이하 ‘법’이라 함) 제2조 제1호에서 규정하는 ‘개인정보’에 해당 하는가? 그리하여 동 법률의 규율대상이 되는가?

<표 1>에 담긴 정보의 내용은 다음과 같은 것이다. 즉, ‘암호화된 주민등록번호를 가진 1966년 8월 30일(생년월일)에 출생한 여자(성별)가 2014년 1월 10일 진해 연세병원 정형외과에서 질병기호 S934의 병으로 대웅제약의 알비스정을 5일치 처방받았다.’는 내용이다. 이 정보의 주체가 ‘누군가 특정한 개인’이라는 점은 분명하다. 이 정보가 만일 그 특정한 개인을 알아볼 수 있는 ‘개인정보’에 해당한다면, 이 정보는 ‘건강에 관한 정보’로서 법 제23조¹⁾의 ‘민감정보’에 해당하게 되고 따라서 정보주체의 사전 동의를 받거나 법령이 처리를 허용하는 경우 외에는 그 처리(수집·이용·제공)에 대해 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해지게 된다(제71조 제3호).

아니면, 이러한 정보는 그 정보주체가 누구인지 알아볼 수 없는 정보이기 때문에 ‘개인정보’에 해당하지 않고, 따라서 그 정보주체의 동의 여하에 관계없이 의약품의 연구나 통계분석 목적을 위해 정보보유자(약국 등)와 통계분석자(데이터마케팅 회사) 사이의 제한적인 공유를 통해 이 정보를 활용하는 것이 현행법의 해석론으로 허용될 것인가?²⁾

-
- 1) 법 제23조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우
 - 2) 본 사안의 쟁점을 법 제18조 제2항 제4호(목적 외 이용·제공)의 해석·적용 문제로 접근하지 않고 제2조 제1호의 해석·적용 문제(‘개인정보 해당 여부’)로 잡은 이유는, 만일 본 사안의 정보가 ‘개인정보’에 해당한다면 법 제23조(민감정보의 처리 제한)의 규정 때문에 제18조 제2항 제4호(목적 외 이용·제공)가 적용될 여지가 없다고 해석되기 때문이다. 제18조 제2항 제4호는 “통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우에, 개인정보처리자는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.”고 규정하고 있다. 법 제18조는 일반의 개인정보 전체를 규율

<표 1> 본 사안의 정보

정보구분	정보내용	처리방식
신원 관련 정보	발행의사 면허번호/성명	가상화코드변환(암호화)
	환자 주민등록번호	
	환자 생년월일	
	환자 성별	
처방전 발급/조제 정보	처방전 발급기관(번호와 명칭) / 발급기관 전화번호 / 진료과 / 처방전 발행일자 / 질병기호	
	조제일자 / 약국서버이름 / 데이터 저장일시/ 데이터 전송일시 / 심평원 청구코드	
약품정보	약품구분 / 약품코드 / 약품명칭 / 제약회사명 / 1회 투약량 / 투여횟수 / 투약일수 / 총투약량 약품단가 / 약품총가격 / 청구액 / 본인부담금	

(2) 「개인정보 보호법」은 “개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.”(제2조 제1호)고 개념정의하고 있다.

본 사안의 정보가 ‘특정의 누군가’에 관한 정보라는 점은 분명하다. ‘특정의 누군가’가 언제 어느 병원에서 어떤 질병기호에 해당하는 병으로 어떤 약을 얼마만큼 처방받았다는 내용의 정보이다. 문제는 ‘암호화된 주민등록번호, 생년월일과 성별’을 가지고 그 특정의 누군가를 식별해낼 수 있느냐 하는 것이다.

물론 이 식별가능성을 판단할 때 본 사안의 정보에 담긴 다른 내용의 정보는 물론이고 이 정보를 활용하는 개인정보처리자가 통상 접근할 수 있는 ‘다른 정보’를 함께 고려해야 할 것이다. 다만, 본 사안에서 이 정보는 일반대중에게 널리 공개된 것이 아니고 의약품정보를 전문적으로 분석·제공하는 민간의 기관에서 통계분석

하는 규정이고, 제23조는 그 중에서도 민감정보를 특별히 보호하는 규정이어서, 특별보호조항인 제23조가 우선 적용된다면 제18조는 적용의 여지가 없게 된다. 의료정보의 활용가능성을 전혀 고려하지 못한 미숙한 입법기술로 인해서 발생하는 문제이다. 입법론적으로는 의료정보의 경우에도 제18조 제2항 제4호가 적용되도록 하는 것이 타당하다. 현행법은 민감정보를 지나칠 정도로 과도하게 보호하고 있다. 일본, 미국, 유럽의 개인정보보호법도 이런 식으로 민감정보를 보호하지는 않는다.

의 목적으로 주고받았다는 점을 사실관계의 전제로 삼는다. 본 사안의 정보를 제공받아 활용하는 민간의 기업은 한국의 질환별 의약품 처방현황을 분석하여 제공하는 KMDI(Korea Medical Data Index)라는 통계자료를 발간하고, 그밖에 처방전에 담긴 정보를 분석하여 다양한 통계자료를 생산하고 그것을 제약회사에게 판매하고 있다고 전제한다.

(3) 위 쟁점은 단순히 법 제2조 제1호의 ‘개인정보’ 개념의 해석·적용에 관한 문제이지만, 좀 더 넓은 관점에서 보면, ‘익명화한 처방정보에 대해 연구·통계 목적으로 전문적인 분석을 자유롭게 허용할 것인가’에 관한 문제이다. 물론 익명화의 방식에 있어서 그 식별성이 쉽게 복원될 수 있는 것이라면 문제가 되겠지만, ‘복호화가 불가능한 암호화된 주민등록번호’는 그 식별성의 복원이 불가능하고, 또한 ‘생년월일과 성별’ 정보는 개인식별정보(identifier)가 아니어서, 이런 수준의 익명화처리라면 ‘연구·통계 목적’으로 일반 공개가 아닌 제한적인 유통이 허용되어야 할 것으로 생각된다.

만일 ‘생년월일과 성별 정보’만이 포함된 환자의 처방정보 내지 의료정보가 특정 개인을 알아볼 수 있는 ‘개인정보’이고 따라서 「개인정보 보호법」의 규율을 받아야 하는 정보라면, 현재 의학계의 임상연구에서 일상적으로 행하고 있는 ‘환자 이름의 머리글자(initial), 생년월일, 성별정보’의 유통 관행은 환자의 동의 범위를 벗어난 것으로 형사처벌의 대상이 될 수 있다.

현재 대학병원과 같은 임상시험기관에서 의사들이 제약회사 등의 의뢰기관으로부터 연구의뢰를 받아 임상시험을 할 때 임상시험대상자(환자)에게서 사전 동의서를 받게 되는데, 그 동의서 설명문에는 ‘환자의 정보는 개인을 알아볼 수 없도록 하여 비밀로 보호된다.’는 취지의 문구가 들어가 있다.³⁾ 그런데 임상시험결과를 보고하는 증례기록서(Case Recording Form)⁴⁾에는 거의 대부분 ‘환자 이름의 머리글자(initial), 생년월일, 성별’이 표기되어 제3자인 시험의뢰기관에 전달된다([별지 1] 증

3) 「의약품 등의 안전에 관한 규칙」(2014. 10. 10. 총리령 제1098호) 별표 4 「의약품 임상시험 관리기준」 제7호 아목 10)은 동의서 설명문에 “시험대상자의 신상을 파악할 수 있는 기록은 비밀로 보호될 것이라는 사실”을 적어야 한다고 규정하고 있다.

4) “증례기록서(Case Report Form, CRF)라 함은 각각의 시험대상자별로 임상시험 계획서에서 요구한 정보를 기록하여 임상시험의뢰자에게 전달할 목적으로 인쇄하거나 전자문서화한 문서를 말한다.” 「의약품 등의 안전에 관한 규칙」(2014. 10. 10. 총리령 제1098호) 별표 4 「의약품 임상시험 관리기준」 제2호 바목.

례기록서 예시 참조). 만일 이렇게 유통되는 ‘환자 이름의 머리글자, 생년월일, 성별’ 정보가 ‘개인을 알아볼 수 있는’ 또는 ‘신상을 파악할 수 있는’ 정보라고 하게 되면, 이러한 정보의 유통은 환자의 동의 범위를 벗어난 것이 되어 불법이 되고, 결과적으로 의료계의 임상시험연구는 현행법 하에서 상당한 타격을 입게 될 것으로 보인다.

현재 의학계의 일반적인 연구관행에서 ‘환자의 생년월일과 성별’은 유의미한 연구학적 통계정보로서 연구에 필수적인 정보이고 이것만으로는 환자 개인을 식별할 수 없다는 인식이 일반화되어 있다. 각 임상시험기관에서 연구윤리 등을 심의하는 임상시험심사위원회(Institutional Review Board, IRB)는 증례기록서에 담기는 ‘환자 이름의 머리글자, 생년월일, 성별’ 정보를 당연한 것으로 인정하고 있다. 이를 통해 유의미한 연구결과를 얻는 경우가 많기 때문이다.

(4) 본 사안 정보의 개인식별성 여부를 판단함에 있어서는 균형 잡힌 이익형량의 관점이 필요하다고 생각된다. 즉, 한편에서는 ‘처방정보의 통계적 분석의 사회적 효용’과 다른 한편에서는 ‘환자의 사생활이익의 보호’를 균형적이고 합리적으로 조정해야 한다. 그러나 아쉽게도 현재 한국에서는 위 양 가치를 미리 구체적으로 조정해 놓은 명확한 규범질서(의료법 등)가 마련되어 있지 않은 상태이다. 그저 일반법인 「개인정보 보호법」을 가지고 이 문제를 풀어야 하는 막연한 상황에 놓여 있다. 그리하여 법적용자들에게 깊은 고민거리를 던져 주고 있다. 본 논문은 그 고민을 함께 해보고자 하는 노력의 일환이다. 이하에서는 ‘개인정보’ 개념에 대한 구체적인 해석·적용에 앞서서 아래 [II.]에서 문제해결에 필요한 기본시각과 관점에 관해 먼저 언급하고자 한다.

II. 개인정보보호법의 존재이유 : ‘보호’와 ‘이용’의 균형

(1) 1980년 이후에 전 세계적으로 새롭게 생겨난 ‘개인정보보호법’이라는 법체계는 개인정보의 ‘보호’만을 도모하고자 하는 것이 아니고 ‘보호’와 ‘이용’의 균형을 도모하고자 하는 법이다. 최근 한국 사회의 일각에서는 개인정보의 ‘절대적 보호’에 치우친 편향된 관점이 과도하게 퍼져 있는 상황이다. 개인정보는 ‘정보주체의 것’이니까 다른 사람은 정보주체의 동의 없이는 원칙적으로 수집·이용·제공할 수 없다는 인식이 상당히 넓게 퍼져 있다. 그러나 ‘정보주체의 동의’는 개인정보 보호법체계에서 ‘원칙’이 아니라 처리의 적법성(lawfulness of processing)을 인정받

는 여러 가지 방법 중의 하나이다. 이는 유럽연합을 비롯한 각국의 개인정보보호법에서 확인할 수 있다.

(2) ‘개인정보의 보호’와 ‘사생활비밀의 보호’는 규범적으로 구별되어야 한다. 제2세대 프라이버시법인 ‘개인정보보호법’은 그 규율의 목적과 대상 및 보호의 방식이 종래의 ‘사생활비밀보호법’과 많이 다르다.

사생활비밀보호법은 ‘公知되지 않은’ 개인의 私的 정보(private information)의 비밀(confidentiality)을 ‘널리 공개’하는 행위를 직접 금지하는 법이다. 이에 비해, 개인정보보호법은 ‘이미 공개되어’ 다른 사람에 의해서 처리되는, 식별되었거나 식별 가능한 개인에 관한 일체의 정보(identified or identifiable personal information)를 예방적으로 보호하는 법이다. 그 보호의 방식은 개인정보의 처리(=수집·이용·가공·제공 등) 자체를 원칙적으로 금지하는 것이 아니라 정당한 업무수행목적의 처리를 허용하되 오·남용되는 일이 없도록 ‘안전하고 투명한 처리’를 목표로 예방적 차원의 보호를 하는 것이다. 이를 위해 처리목적을 미리 분명하게 밝히게 하고(목적명확성의 원칙), 원칙적으로 그 목적 범위 내에서 이용 또는 공유하게 하며(이용제한의 원칙), 또 그 처리과정에 정보주체의 참여(열람·정정·삭제 등)를 보장하는(참여의 원칙) 방식이다.⁵⁾ 사생활비밀보호법이 구체적인 법익(사생활비밀)의 ‘침해금지법’이라고 한다면, 개인정보보호법은 ‘위험예방법’의 성격을 가진다. 때문에 개인정보보호법은 정보주체에게 그 처리에 대한 전면적인 통제권을 주고자 하는 것이 아니다. ‘개인정보자기결정권’ 내지 ‘개인정보보호권’을 그런 내용으로 오해해서는 안 된다. 만일 정보처리의 전 과정에 정보주체의 동의를 요구하는 것이 개인정보자기결정권 내지 개인정보보호권의 내용이라고 오해한다면, 그것은 개인정보보호법의 목적과 성격을 잘못 이해한 것이다. 이 점은 개인정보보호법을 해석함에 있어서 반드시 유의해야 될 대목이다.

5) 사생활비밀보호법의 규율방식이 ‘은둔 모델’(seclusion model)이라고 한다면, 개인정보보호법은 ‘참여 모델’(participation model)이라고 할 수 있다. 양 모델의 차이점에 관한 상세한 논의는 이인호, “제2세대 프라이버시보호법으로서의 개인정보보호법에 대한 이해”, 사법 제8호 (사법발전재단, 2009) 참조.

	종래의 사생활비밀보호법	새로운 개인정보보호법
규율목적	실제로 발생한 해악(사생활침해)에 대해 제재를 가함 ➡ 사후규제의 침해금지법	업무수행과정에서 이루어지는 개인정보처리의 오·남용을 사전에 막음으로써 정보주체의 다양한 법익이 침해될 수 있는 위험(risk)을 예방하고자 하는 것임 ➡ 위험관리를 통한 안전한 이용 (사전규제의 위험예방법)
규율대상	사생활평온이나 비밀을 깨뜨리는 행위	개인정보DB의 형태로 처리되는 개인정보의 처리과정(=수집·이용·제공 등)
규율방식	법익침해의 기준을 설정하고 기준위반에 대해 민사적 또는 형사적 제재를 가함	<ul style="list-style-type: none"> - 합법적인 개인정보처리의 기준 설정 - 개인정보처리의 절차적 요건(목적명시/품질관리/고지/보고 요건)의 설정 - 정보처리과정의 정보주체의 참여 보장 - 독립적인 감독기구에 의한 처리기준의 준수여부 감독/컨설팅/민원과 고충의 처리/교육

(3) 요컨대, 개인정보보호법은 개인정보의 ‘보호’의 가치만을 도모하는 것이 아니고 ‘이용’의 가치 또한 충분히 고려하면서 양 가치의 ‘적절한 균형’을 도모하는 법이다. 이는 모든 국가의 개인정보보호법이 추구하는 공통된 방향이다.⁶⁾

- 6) 외국의 모든 개인정보보호법은 이 점을 목적조항에서 명시하고 있다. 세계 각국 개인정보보호법의 입법모델이 된 **1995년의 유럽연합 개인정보보호지침(95/46/EC)**은 제1조(이 지침의 목적)에서 두 가지 입법목적을 다음과 같이 명시하고 있다: “1. 이 지침에 따라서, 회원국들은 자연인의 기본적인 권리와 자유, 특히 개인정보의 처리와 관련한 프라이버시권(right to privacy with respect to the processing of personal data)을 보호하여야 한다. 2. 회원국들은 위 1.에 근거해서 주어지는 보호와 관련된 이유를 들어 회원국 사이의 개인정보의 자유로운 유통(the free flow of personal data between Member States)을 제한하거나 금지해서는 아니 된다.” **일본**의 기본법이면서 민간부문의 일반법인 「**개인정보의 보호에 관한 법률**」 제1조(목적)도 “이 법률은 고도정보통신사회의 진전에 따라 개인정보의 이용이 현저하게 확대되고 있는 점에 비추어, 개인정보의 적절한 취급과 관련하여 기본이념 및 정부에 의한 기본방침의 작성 기타 개인정보의 보호에 관한 시책의 기본이 되는 사항을 정하고, 국가 및 지방자치단체의 책무 등을 명확히 함과 동시에, 개인정보를 취급하는 사업자가 준수하여야 할 의무 등을 규정함으로써 개인정보의 유용성을 배려하면서도 개인의 권리이익을 보호하는 것을 목적으로 한다.”고 규정하고 있다. 또한 **독일**의 공공·민간부문을 포괄하는 일반법인 연방의 「**개인정보 보호법**」(Datenschutzgesetz) 제1조도 개인정보가 저장, 전달, 수정 및 처리되는 과정에서 잘못 이용되지 않도록 함으로써 보호되어야 할 다른 개인의 권리와 이익이 침해되는 것을 막

어떤 사회든지 개인에 관한 정보(개인정보)의 수집·이용·공유를 전제로 해서 여러 사회적 기제가 작동하고 있다. 비근한 예로, 법원이 재판을 하기 위해서는 원·피고에 관한 정확한 개인정보를 수집·이용·공유해야 하고, 의료사고소송의 경우 병원 측의 소송대리인은 환자의 민감한 진료정보를 공유·이용해야만 소송수행이 가능해진다(물론 이때의 공유는 ‘공개’가 아니라 의뢰인과 대리인 사이의 ‘제한적 공유’이다).

또한 본 사안에서처럼 의약 분야에서 통계목적이나 연구목적을 위하여 처방정보를 수집하여 분석하는 것은 의약의 발전과 더 나은 의료정책의 개발이라는 중요한 공익 실현에 필요한 일이다. 나아가 이러한 정보의 수집과 분석이 제약회사의 정당한 마케팅 목적에 활용되는 경우가 있는데 그러한 마케팅 목적 또한 적절한 자원배분이라는 사회적 효용을 가지고 있다. 이 점은 아래에서 살피는 미국 연방대법원의 2011년의 위헌판결에서 확인된다.

(4) 2011년에 미국 연방대법원은 *Sorrel v. IMS Health Inc.* 판결에서, 개별 의사의 처방행태(prescribing practices)를 드러내는 처방전 정보를 의사의 동의 없이 마케팅 목적으로 판매하거나 이용하는 행위를 금지하는 버몬트(Vermont)주의 법률을 위헌이라고 판결하였다. 미국에서는 처방전에 담긴 의사 개인의 처방행태에 관한 정보는 의료정보보호법(HIPAA)⁷⁾의 보호대상이 아니며, 약국체인들은 이들 정보를 의사의 동의 없이 IMS와 같은 데이터분석회사(data mining company)에 판매하고, 데이터분석회사는 의사 개인별 분석정보를 제약회사에 판매하며, 제약회사는 이 분석정보를 활용하여 의사 개인별 판촉활동(detailing)을 해 왔다. 버몬트 주의 새로운 법률은 이러한 관행을 금지시킨 것이다. 이 사건에서 미연방대법원은 주의 법률이 데이터분석회사와 제약회사의 판촉활동, 즉 표현의 자유(freedom of speech)를 침해하여 위헌이라고 판결하였다.⁸⁾ 이 사건에서 버몬트주는 위 법률이 의료비밀(medical privacy)을 보호하기 위해서 불가피하고 또 공중보건(public healthcare)을 증진시키는데 기여한다고 주장했지만, 연방대법원은 이를 받아들이지 않았다.

위 미국의 사례는 본 사안의 분석에 있어서도 示唆하는 바가 크다고 생각된다.

기 위한 것이 이 법의 목적임을 밝히고 있다.

7) 정식 명칭은 「건강보험 이동성 및 책임에 관한 법률」(Health Insurance Portability and Accountability Act, HIPAA)임. 1996년에 제정됨.

8) *Sorrel v. IMS Health Inc.*, 131 S.Ct. 2653 (2011).

미국의 경우에는 의사 개인의 實名의 처방정보라도 법적 제약이나 정보주체인 의사의 동의 없이 자유롭게 사회적 유통이 허용되고 또 그것이 헌법적으로 보호받고 있는 것을 보면, 비록 미국의 규범상황을 한국이 쫓아가야 할 필연성은 반드시 없지만, 적어도 사회적으로 필요한 개인정보의 유통과 이용의 가치를 무시해서는 안 된다는 시사점을 제공해 준다.

(5) 본 사안의 경우처럼 통계분석 목적으로 익명처리에 의한 제한적인 정보공유를 ‘개인정보의 보호’라는 명분으로 무조건 좌악시하는 것은 곤란하다. 이는 「개인정보 보호법」을 해석하는 균형 잡힌 시각이라고 볼 수 없다. 최근 우리 사회에서는 개인정보에 대한 ‘보호’의 가치를 절대화하는 경향이 있다. 마치 ‘개인정보’를 종래의 ‘사생활비밀’과 같이 취급하여, 일체의 개인정보에 대한 통제권이 정보주체에게 원천적으로 귀속되어 있는 것처럼 오해하고 있다. 그리하여 정보주체의 동의 없는 수집·이용·제공을 원칙적으로 불법으로 보려는 경향이 있다. 이러한 오해의 경향은 2005년의 헌법재판소의 한 결정에 의해 증폭되었다. 헌법재판소는 ‘주민등록지문정보DB 사건’⁹⁾에서 처음으로 ‘개인정보자기결정권’이라는 새로운 독자적인 기본권을 인정하였는데, 마치 이 결정이 정보주체에게 절대적 통제권을 인정한 것처럼 오해하고 거기에 더하여 기본권의 對私人效라는 또 다른 오해의 관점이 어우러져, 민사관계에서도 헌법상의 기본권인 개인정보자기결정권이 바로 적용되는 것처럼 잘못 이해되고 있다.¹⁰⁾

그러나 이러한 오해와 편향된 시각은 ‘사전규제의 위험예방법’인 개인정보보호법의 존재이유를 망각하거나 무시하는 태도이다. 개인정보보호법의 존재이유는 개인정보 그 자체를 절대적으로 보호하려는 것이 아니고, 개인정보의 ‘보호’와 ‘이용’의 적절한 균형을 도모하는 데에 있다. 아래에서는 이러한 기본적 이해를 전제로 해서 「개인정보 보호법」 제2조 제1호의 ‘개인정보’ 개념에 대한 해석론을 전개하고자 한다.

9) 헌재 2005. 5. 26. 99헌마513등 (주민등록 지문정보DB 사건) [6(합헌) : 3(위헌)].

10) 이러한 오해의 원인과 내용 및 그 비판에 대해서는 이인호, “변호사의 직업적 개인정보에 대한 이용과 보호의 법리: 로마켓 변호사평가정보 사건(2008다42430)에 대한 평석을 겸하여”, 언론과 법 제11권 제2호, 한국언론법학회, 2012 참조.

Ⅲ. 개인식별성에 관한 주요 외국 입법례의 비교

1. 보호대상이 되는 ‘개인정보’의 필수적 개념요소 : 個人識別性

「개인정보 보호법」 제2조 제1호는 “개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.”고 규정하고 있다.¹¹⁾ 일반적으로 개인정보보호법에서 보호하는 ‘개인정보’는 ‘특정 개인에 관한 일체의 정보’를 의미한다. 특정 개인에 ‘관한’ 것이면 모든 형태와 내용의 정보가 여기에 해당된다. 따라서 보호의 대상은 매우 광범위하다.

물론 이때 보호의 대상이 되는 정보는 ‘개인식별성’(identification)을 갖추어야 한다. 즉 그 정보가 누구에 관한 것인지 그 정보주체를 ‘알아볼 수 있어야’ 한다. 누구에 관한 것인지를 알 수 없는 개인정보는 개인정보보호법의 보호대상에서 제외된다. 왜냐하면 법이 종국적으로 보호하고자 하는 것은 ‘정보’ 그 자체가 아니라 그 정보의 오·남용으로 인해 침해될 특정 개인(정보주체)의 권리나 이익이기 때문이다. 누구에 관한 것인지 알 수 없는 개인정보는 오·남용이 있더라도 그로 인해 어느 누구의 권리나 이익도 침해되는 바가 없기 때문이다.

어느 나라의 개인정보 보호법이든 보호대상이 되는 ‘개인정보’를 정의할 때 ‘개인이 식별되는(identified) 또는 식별가능성이 있는(identifiable) 정보’라는 개념요소를 필수적으로 담고 있다. 우리나라 법의 ‘개인정보’ 개념에 대한 해석론에 참고가 되는 주요 외국법상의 개념정의를 간략하게 살펴보고자 한다.

2. 주요 외국법의 ‘개인정보’ 개념에 대한 비교법적 분석

(1) 미국의 공공부문 개인정보 보호법인 「프라이버시법」(Privacy Act)은 보호대상이 되는 ‘개인기록’(personal record)을 다음과 같이 정의하고 있다: “개인기록

11) 온라인 개인정보보호법인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호도 거의 동일한 개인정보의 개념을 규정하고 있다: “개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 부호·문자·음성·영상 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.”

(record)이라 함은 행정기관이 보유하는 개인에 관한 정보(information about an individual)의 개개 항목 또는 그 집합을 말한다. 그 기록에는 그 개인의 교육, 금전적 거래, 병력(病歷), 전과(前科) 또는 취업경력에 관한 정보가 담기는데 이에 한정되지 않는다. 그리고 그 기록에는 당해 개인의 이름(name), 또는 식별번호나 식별부호(the identifying number or symbol) 또는 그밖에 당해 개인에게 고유한 식별자(other identifying particular assigned to the individual) 예컨대 지문(指紋)·성문(聲紋)·사진과 같은 것이 포함되어 있어야 한다.”¹²⁾ 따라서 이 법률은 이름을 비롯한 고유 식별자(identifying particular or identifier)를 통해 개인 식별이 되는(identified) 정보만을 보호대상으로 하고 있다.

(2) 한편, 미국의 의료정보보호법(HIPAA)에서 ‘보호를 받는 의료정보’(protected health information; PHI)는 ‘개인을 식별할 수 있는 의료정보’(individually identifiable health information)에 한정된다. 이 법률의 개념정의는, “개인을 식별할 수 있는 의료정보”란 “(i) 개인을 식별하거나(identifies the individual) 또는 (ii) 그 정보가 개인을 식별하는데 사용될 수 있다고 믿을 만한 합리적인 근거가 있는(there is a reasonable basis to believe that the information can be used to identify the individual) 의료정보를 의미한다.”고 규정하고 있다.¹³⁾ 이 개념정의에서 (ii)는 ‘식별가능성이 있는(identifiable) 정보’를 가리킨다. 즉, 개인이 바로 식별되지는 않지만 ‘식별가능성이 있는 정보’까지 보호대상으로 삼고 있다. 그런데 ‘식별가능성’의 판단기준으로 ‘그 정보가 개인의 식별에 사용될 수 있다고 믿을 만한 합리적인 근거가 있을 것’을 제시하고 있다.

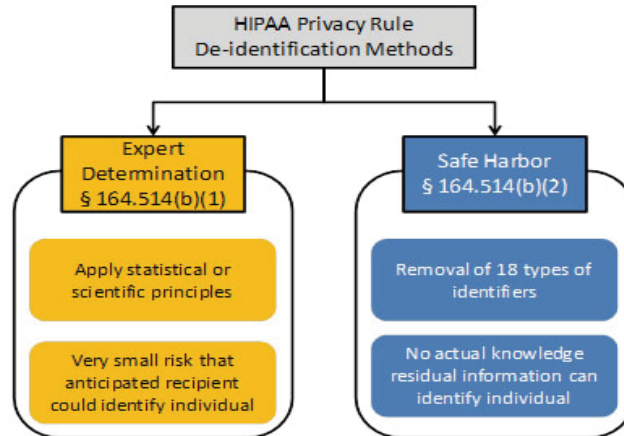
그리고 이 법률을 구체화하는 법규명령인 「프라이버시 규칙」(HIPAA Privacy Rule)¹⁴⁾은 식별가능성이 없거나 매우 약한 의료정보가 연구나 조사 목적에 매우 유용하다는 점을 인정하여, 규칙이 정하는 일정한 식별자들(identifier)을 제거한 두 가지 유형의 의료정보 즉 ‘비식별화된 의료정보’(de-identified health information)와

12) 5 U.S.C. §552a(a)(4). 「the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.」

13) 42 U.S.C. § 1302d(6). 원문은 <<http://www.law.cornell.edu/uscode/text/42/1302d>> 참조.

14) 「HIPAA 프라이버시 규칙」은 연방 법규명령집(CFR) 제164부(Part 164)에 담겨 있다.

‘제한적인 데이터집합’(limited data set)을 설정하고, 전자에 대해서는 전면적인 규율면제(즉 규율대상에서 전적으로 제외)를, 후자에 대해서는 조건적 규율면제를 인정하고 있다.¹⁵⁾ 이에 관해 좀 더 구체적인 설명을 붙이고자 한다.



<그림 1> 「프라이버시 규칙」이 규정하는 비식별화(de-identification)의 두 가지 방식

먼저, 「프라이버시 규칙」은 ‘비식별화된 의료정보’(de-identified health information)를 보호대상에서 명시적으로 제외하여 이런 정보의 자유로운 이용 및 제공을 허용하고 있다.¹⁶⁾ 이 규칙에 따르면, **비식별화(de-identification)**에는 **두 가지 방식**이 허용된다. ❶ **하나**는, 경험 있는 통계전문가가 통계적 혹은 과학적 원칙을 적용하여 예상되는 정보수령자(anticipated recipient)가 개인을 알아볼 수 있는 위험성(risk of re-identification)이 ‘**매우 적다**’(very small)는 결정을 정식으로 내리는 경우이다.¹⁷⁾ 이를 ‘전문가결정 방식’(expert determination method) 혹은 ‘통계적 방식’(statistical method)이라고 부른다. ❷ 또 **다른 하나의 대안적 방식**은, 규칙에서 명시한 18가지의 식별자(identifier)를 제거하고 그리고 남은 정보가 그 자체로 혹은 다른 정보와 결합해서 개인 식별에 사용될 수 있다는 점을 정보처리자(규율대상기관)가 실제로

15) Center for Democracy & Technology(미국 비영리시민단체), “Encouraging the Use of, and Rethinking Protections for De-Identified (and Anonymized) Health Data”(June 2009), p. 1. 원문은 <https://cdt.org/files/pdfs/20090625_deidentify.pdf> 참조.

16) HIPPA Privacy Rule, 45 C.F.R. §§164.502(d)(2), 164.514(a) 및 (b).

17) 45 C.F.R. §164.514(b)(1).

인식하지 못한 경우이다.¹⁸⁾ 이를 ‘피난처 방식’(safe harbor method)이라고 한다.¹⁹⁾ 이 피난처 방식에서 규정하는 18가지의 식별자는 아래의 <표 2>와 같다.

<표 2> 피난처 방식에서 규정하는 18가지 식별자

1. Names (이름)	11. Certificate/license numbers (신분증/면허 번호)
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code (주(州) 단위 미만의 지리적 세부정보. 다만 우편번호의 앞 3자리는 제외됨)	12. Vehicle identifiers and serial numbers, including license plate numbers (차량 번호)
3. All elements of dates (except year) for dates directly related to an individual, including birth data, admission date, discharge date, date of death (태어난 날짜, 사망날짜 등 개인과 직접 관련 되는 날짜. 다만 연도는 제외됨)	13. Device identifiers and serial numbers (장치식별번호)
4. Telephone numbers (전화번호)	14. Web Universal Resource Locators (URLs) (웹페이지주소)
5. Fax numbers (팩스번호)	15. Internet Protocol (IP) address numbers (IP주소)
6. Electronic mail addresses (이메일주소)	16. Biometric identifiers, including finger and voice prints (指紋과 聲紋을 포함하는 생체식별자)
7. Social security numbers (사회보장번호)	17. Full face photographic images and any comparable images (전면의 얼굴이미지)
8. Medical record numbers (진료기록번호)	18. Any other unique identifying number, characteristic, or code, except the unique code assigned by the investigator to code the data (기타 유일한 식별번호, 특징 또는 부호. 다만 조사자가 그 데이터를 암호화하기 위해 할당한 고유 코드는 제외됨)
9. Health plan beneficiary numbers (건강보험수혜자번호)	
10. Account numbers (계좌번호)	

다음으로, 「프라이버시 규칙」은 부분적인 규율면제를 받는 의료정보의 유형으로 ‘제한적인 데이터집합’(limited data set)을 설정하고 있다.²⁰⁾ 이 유형의 정보는 제한

18) 45 C.F.R. §164.514(b)(2).

19) 이 설명에 관한 내용의 원문은 미국 보건복지부(Department of Health and Human Services)의 의료정보프라이버시 사이트(Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule) http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#_ednref4 참조.

적인 요건 하에서 정보주체(환자)의 동의나 허가 없이 이용하고 또 제공할 수 있다. 「프라이버시 규칙」은 두 가지 요건을 규정하고 있다. 하나는, 위 피난처 방식에서 규정한 18가지 식별자 중 ‘직접적 식별자’(direct identifiers)에 해당하는 16가지 식별자를 제거해야 한다.²¹⁾ 위 16가지 직접적 식별자에 해당하지 않는 ‘간접적 식별자’(indirect identifier)는 연구나 조사 목적에 때때로 필요한 것으로서 생년월일(birth data), 치료나 처방일자(dates of treatment), 일부 지리적 정보(우편번호, 주(州), 도시, 타운)가 여기에 해당된다.²²⁾ 그리고 또 하나의 요건은, 이러한 데이터를 제공 받는 자와 ‘데이터이용계약’(data use agreement)을 체결해야 한다. 이 계약에는 허용되는 데이터 이용 및 제공 목적(연구, 공중보건, 또는 치료)을 명시하고, 데이터를 이용하거나 수령할 수 있는 자의 범위를 제한하며, 그리고 그 데이터의 식별성을 복원(re-identification)하지 않는다는 약속이 담겨야 한다.²³⁾

이상을 정리하면, 미국의 의료정보보호법체계 하에서는 규칙이 정하는 18가지 식별자(identifier)가 제거된 환자의 처방전 정보(de-identified health information)는 법의 규율로부터 완전히 면제되어 누구나 자유롭게 이용 및 제공할 수 있다. 그리고 16가지 직접적 식별자(direct identifier)를 뺀 간접적 식별자[생년월일, 치료나 처방일자, 일부 지리적 정보(우편번호, 주(州), 도시, 타운)]는 처방전의 다른 정보와 함께 일정한 목적(연구, 공중보건, 또는 치료)을 위해 데이터이용계약의 체결이라는 조건 하에 환자의 동의 없이 자유롭게 이용 및 제공될 수 있다.

(3) 유럽연합의 개인정보보호지침(95/46/EC) 제2조는 “개인정보”(personal data)라 함은 “개인이 식별되는(identified) 또는 식별이 가능한(identifiable) 자연인(natural

20) 45 C.F.R. §164.514(e).

21) 45 C.F.R. §164.514(e)(2). 16가지 직접적 식별자(direct identifiers) - (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

22) Center for Democracy & Technology, 앞의 글(각주 15), p. 2.

23) 45 C.F.R. §164.514(e)(3)(4).

person)에 관한 일체의 정보(any information)를 말하며; 식별이 가능한 사람(identifiable person)이라 함은 직접 또는 간접적으로(directly or indirectly) 식별이 될 수 있는(can be identified) 사람을 가리키는데, 특히(in particular) 개인식별번호(an identification number) 혹은 그의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 동일성(identity)을 고유하게 나타내는 하나 또는 그 이상의 요소를 참조하여(by reference to) 식별될 수 있다.”²⁴⁾고 규정하고 있다. 이 지침은 식별가능성의 판단방법으로 개인의 동일성을 나타내는 고유식별자(unique identifier)를 참조할 것을 특별히 지시하고 있다.

(4) 영국의 개인정보 보호법(Data Protection Act 1998)은 “개인정보”(personal data)라 함은 “살아 있는 개인에 관한 정보로서, (a) 그 정보로부터, 또는 (b) 그 정보와 그 외 정보처리자(data controller)가 보유하고 있거나(is in the possession) 또는 보유하게 될 것 같은(is likely to come into the possession) 다른 정보를 결합해서 그로부터 개인이 식별될 수 있는(can be identified) 것을 말한다.”²⁵⁾고 규정하고 있다.

영국의 법률은 고유식별자를 특별히 언급하고 있지 않으며, 다만 (a) 그 정보 자체로부터 개인이 식별되는(identified) 경우와 (b) 그 정보 자체로부터 식별되지는 않지만 다른 정보와 결합해서 식별이 가능한(identifiable) 경우를 규정하고 있다. 그리고 식별가능성을 판단하는 데 필요한 ‘다른 정보’란 ‘개인정보처리자’가 보유하고 있거나 또는 보유할 가능성이 있는 정보를 의미하는 것임을 분명히 하고 있다.

(5) 마지막으로, 한국의 개념정의와 가장 유사한 일본의 「개인정보의 보호에 관한 법률」 제2조 제1항은 “이 법률에서 「개인정보」라 함은 “생존하는 개인에 관한 정보로서, 당해 정보에 포함되어 있는 성명, 생년월일 그 밖의 기술(記述) 등에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 조합(照合)〔서로 맞추어 봄〕할 수 있고, 그로써 특정의 개인을 식별할 수 있게 되는 것을 포함한다)을 말한다.”²⁶⁾고 규정하고 있다.

24) Directive 95/46/EC §2(a).

25) Data Protection Act 1998 Section 1(1) : “personal data means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.”

일본의 법률도 위 영국과 마찬가지로 ‘성명, 생년월일 그 밖의 기술(記述) 등’에 의하여 그 정보 자체로 식별되는(identified) 경우와 다른 정보와 용이하게 照合하여 식별이 가능한(identifiable) 경우를 포함하고 있다. 일본의 개념정의에서는 ‘생년월일’을 식별자의 하나로 제시하고 있지만, 후생노동성과 경제산업성이 2014년에 공동으로 고시한 「개인정보 보호법에 대한 경제산업 분야를 대상으로 한 가이드라인」²⁷⁾에서는 ‘생년월일’만으로는 개인정보로 인정되지 않고 성명이 함께 조합되어야 한다는 점을 분명히 하고 있다. 즉 ‘개인정보에 해당하는 사례’의 하나로 “생년월일, 연락처(주소·거소·전화번호·이메일주소), 회사에서의 직위 또는 소속에 관한 정보에 대해서는, 그것들과 본인의 성명이 조합된 정보”를 예시하고 있다.²⁸⁾ 또한 위 가이드라인은 “다른 정보와 용이하게 照合할 수 있는”이라 함은 “예를 들어 통상의 작업범위에서 개인정보데이터베이스에 접근해서 조합(照合)할 수 있는 상태를 말하며, 다른 사업자에게 조회(照會)[물어서 알아봄]해야 하는 경우 또는 당해 사업자 내부에서도 취급부문이 다른 경우 등 조합(照合)이 곤란한 상태를 제외한다.”²⁹⁾고 해설하고 있다.

IV. 「개인정보 보호법」의 해석론 : 개인식별성의 세 가지 판단방법

(1) 「개인정보 보호법」 제2조 제1호는 그 개념규정에서 개인식별성(identification)을 판단하는 세 가지 방법을 제시하고 있는 것으로 판단된다. 그 방법은 첫째, 고유

26) “この法律において 「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む)をいう ”³⁰⁾

27) 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成26年12月12日 厚生労働省・経済産業省告示第4号). 원문은 다음의 URL에서 확인할 수 있다.
<http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf>

28) 【個人情報に該当する事例】 <출전: 위 가이드라인, 3면>

事例1) 本人の氏名

事例2) 生年月日、連絡先(住所・居所・電話番号・メールアドレス)、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報

事例3) 防犯カメラに記録された情報等本人が判別できる映像情報

29) 「他の情報と容易に照合することができ、…」とは、例えば通常の作業範囲において、個人情報データベース等にアクセスし、照合することができる状態をいい、他の事業者への照会を要する場合等であつて照合が困難な状態を除く ”<출전: 위 가이드라인 2면>

식별자를 통한 판단 방법, 둘째, 고유식별자는 없지만 해당 정보에 포함된 다른 요소정보들을 종합적으로 고려하여 개인을 식별하는 방법, 셋째, 정보처리자가 합리적으로 접근할 수 있는 ‘다른 정보’와 쉽게 결합하여 개인을 식별하는 것이다.

(2) 첫째, 고유식별자(unique identifier)를 통한 판단이다. 법은 “성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보”라고 규정하고 있다. 즉, 그 정보에 개인의 고유식별자가 담겨 있으면 그 정보는 개인이 식별되는 정보(identified information)로서 그 자체로 보호대상이 되는 개인정보가 된다. 법률은 고유식별자로 세 가지(“성명, 주민등록번호 및 영상”)를 명시적으로 들면서 그 뒤에 ‘기타’의 의미를 지니는 “등”을 제시하고 있다. 한편 정보통신망법은 “성명·주민등록번호 등”을 고유식별자로 제시하고 있다. 여기서 본 사안과 관련하여 두 가지 쟁점이 제기될 수 있다.

① 첫 번째 쟁점은 법문의 “등”에 생년월일이나 성별이 포함된다고 볼 것인가 하는 점이다. 그러나 생년월일과 성별은 그 자체로는 개인에게 고유한 식별자로 볼 수 없고, 따라서 법문의 “등”에 포함되지 않는다고 판단된다. 통상 입법기술에 있어서 ‘기타’의 의미를 지니는 ‘등’은 앞에 열거된 것과 동등한 규범적 가치를 가진 것이거나 혹은 그에 준하는 규범적 의미를 지닌 것을 지칭할 때 사용하게 된다. ‘성명, 주민등록번호, 영상’은 그 자체로 개인에게 고유한 식별자이지만, ‘생년월일’이나 ‘성별’은 그와 동등하거나 그에 버금가는 고유식별성이 인정되지 않는다고 판단된다.

위에서 살핀 바와 같이, 일본의 후생노동성과 경제산업성의 공동 가이드라인에서도 ‘생년월일’과 ‘성명’이 함께 조합되어야만 개인정보로 인정된다는 점을 분명히 하고 있다. 또한 미국의 「프라이버시법」(Privacy Act)은 ‘이름이나 식별번호’ 외에 기타의 고유식별자로서 ‘지문(指紋, finger print), 성문(聲紋, voice print), 사진(photograph)’을 제시하고 있다. 그리고 미국의 「의료정보보호법 프라이버시 규칙」은 ‘환자의 생년월일, 치료 혹은 처방일자, 일부 지리적 정보(우편번호, 주(州), 도시, 타운)’는 ‘간접적 확인자’(indirect identifier)로서 연구나 조사 목적에 때때로 필요하다는 이유 때문에 일정한 요건(정보이용계약의 체결) 하에 자유로운 이용과 제공을 허용하고 있다. 요컨대, ‘생년월일’과 ‘성별’은 그 자체로는 ‘고유식별성’이 인정되지 않는다고 할 것이다.

② 두 번째 쟁점은, 고유식별자인 ‘주민등록번호’를 삭제 또는 암호화하거나 혹

은 ‘영상이나 음성’의 경우 모자이크처리 혹은 음성변조의 방식으로 비식별(非識別)처리(de-identification)한 경우에 비식별화된 고유식별자를 규범적으로 어떻게 평가할 것인가 하는 점이다. 구체적으로 본 사안에서는 주민등록번호를 암호화하여 처리하고 있는 경우에 그 ‘암호화된 주민등록번호’를 법률의 고유식별자를 가리키는 ‘주민등록번호’와 동등하게 취급할 것인가 하는 점이다.

생각건대, 양자는 동등하게 취급할 수 없을 것으로 판단된다. 평문(平文)의 주민등록번호와 암호화된 주민등록번호는 개인식별자에 관한 법률규정의 해석·적용에 있어서 규범적으로 전혀 다르게 평가되어야 할 것으로 보인다. 암호화된 주민등록번호에는 개인을 식별하는 기능이 없기 때문이다. 요컨대, 통상적인 기술수준에서 암호화된 주민등록번호는 더 이상 법이 규정하는 고유식별자로 인정될 수 없다고 할 것이다. 그렇다면 이 사안의 정보 중 암호화된 주민등록번호, 생년월일, 성별은 고유식별자로 인정될 수 없고, 따라서 법이 규정하는 첫 번째 방법으로는 개인을 식별할 수 없다고 할 것이다.

(3) 다음으로, 해당 정보에 고유식별자는 없지만 그 정보에 포함된 다른 요소정보들을 종합적으로 고려하여 개인을 식별하는 방법이다.

위 <표 1>에 담긴 본 사안의 정보는 그 요소정보들을 종합하면 다음과 같은 내용으로 구성되어 있다. 즉, ‘1966년 8월 30일(생년월일)에 출생한 여자(성별)가 2014년 1월 10일 진해연세병원 정형외과에서 질병기호 S934의 병으로 대웅제약의 알비스정을 5일치 처방받았다.’는 내용이다. 이런 내용의 정보의 주체는 ‘누군가 특정한 개인’이라는 점은 명백하다. 그리고 그 특정한 개인의 입장에서 보면 이 정보가 자신에 관한 것이라는 것을 인식할 수 있을 것이다.

그러나 법률상 보호대상이 되는 ‘개인정보’는 그 특정한 개인을 ‘알아볼 수 있는’ 것이어야 한다. 개인의 ‘특정성’은 개인정보 개념의 구성요소이지만 그것만으로는 개인정보의 요건을 충족하기에 부족하고, 개인의 ‘식별성’이 있어야만 보호의 대상이 되는 ‘개인정보’에 해당하게 된다. 그리고 ‘알아볼 수 있다’는 것은 정보주체의 입장에서가 아니라 ‘다른 사람’, 즉 정보처리자나 일반인이 그 정보주체를 알아볼 수 있다는 것을 의미한다. 위에서 살핀 주요 외국의 개념정의에서도 모두 마찬가지로 규정함으로써 정보주체인 특정 개인을 식별의 ‘객체’로 규정하고 있을 뿐 ‘주체’로 보고 있지 않다. 다른 사람들이 그 정보가 누구의 것인지 모른다면 정보처리

와 관련해서 생겨날 수 있는 정보주체의 권리와 이익에 대한 위협은 없다고 보아야 할 것이다. 혹시라도 본인 혼자서 느끼는 사소한 감정의 변화까지도 보호하려는 것이 개인정보 보호법의 입법취지는 아니기 때문이다. 즉, 법은 개인정보처리의 오·남용으로 인해 타인과의 관계 속에서 발생할 수 있는 정보주체의 권리와 이익을 보호하고자 하는 데에 그 입법취지가 있다.

그렇다면 본 사안에서도 정보처리자 또는 일반인의 관점에서 이 사안 정보의 정보주체를 식별해내어야 하는데, 이 사안의 정보만으로는 그 정보주체를 식별하는 것이 거의 불가능해 보인다. 왜냐하면, 생년월일과 성별만으로는 특정 개인을 식별할 수 없기 때문이다.

우리나라의 연도별 출생아 수는 아래 <표 3>과 같다. 출산율이 저조한 최근 11년 동안의 평균으로 계산하더라도 한 해에 약 47만(469,872) 명이 태어나는데, 남녀 비율을 1:1로 가정하면 남녀 각각 23만 5천명이고, 1년 365일 중 특정일에 태어나는 사람은 평균으로 남녀 각각 약 643명 정도가 된다. 요컨대, 생년월일과 성별을 가지고 이 사안 정보의 주체가 누구인지 식별하는 것은 불가능한 것으로 판단된다.

<표 3> 연도별 출생아수 [단위 : 천명]³⁰⁾

연도	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
출생아수	492.1	490.5	472.8	435	448.2	493.2	465.9	444.8	470.2	471.3	484.6

한편, 환자의 생년월일과 성별은 「약사법」에 따른 의약품 유해사례 보고서상에 익명으로 입력되는 환자정보에도 들어가 있다. 현행 「약사법」과 「의약품 등의 안전에 관한 규칙」은 의약품 유해사례 보고제도를 두고 있는데, 약국 개설자와 의료기관 개설자는 의약품 등으로 인하여 발생하였다고 의심되는 유해사례를 식품의약품안전처장이 정하는 바에 따라 의약품안전관리원장에게 보고하도록 하고 있다(약사법 제68조의8 제2항, 의약품 등의 안전에 관한 규칙 제84조 제2항). 이때 작성되는 ‘의약품등 유해사례 보고서’³¹⁾에는 필수항목으로 되어 있는 ‘환자정보’의 경우 환자의 ‘이름’은 머리글자로 표시하고, ‘생년월일과 성별’을 표시하도록 하고 있

30) 출처 : 통계청, 「2013년 출생통계, 국가승인통계 제10103호 출생통계」

31) 「의약품 등 안전성 정보관리 규정」(2014. 2. 20. 식품의약품안전처고시 제2014-97호) 제8조 [서식 1] 의약품등 유해사례 보고서.

으며, 그밖에 환자의 병력, 약물사용력, 유해사례의 내용 등을 상세하게 기재하도록 하고 있다(아래 <서식 1> 참조).

<서식 1> 「약사법」에 의한 의약품 등 유해사례 보고서

◆ 작성 시 참고사항을 확인하시고, 필수사항^(*) 외에 불분명한 사항은 기입하지 않으셔도 되며, 기입란이 부족한 경우에는 별지를 이용하여 주십시오.

의약품 등 유해사례 보고서					
보고서 정보		보고자 관리번호/제목 ³⁾ : _____		한국의약품안전관리원 관리번호: (자동 생성)	
발생인지일 ⁴⁾ : ____년 ____월 ____일		신속보고 ⁵⁾ 여부: <input type="checkbox"/> 예 <input type="checkbox"/> 아니오		보고일: (자동 생성)	
<input type="checkbox"/> 최초보고 <input type="checkbox"/> 추적보고 ⁶⁾ (이전 보고의 관리번호/제목: _____ 추적보고 사유: _____)					
참조보고 ⁷⁾ (관리번호/제목): _____ <div style="float: right;">중대한 유해사례인 경우(해당되는 경우 모두 표시)</div>					
의약품문인에 의하여 확인된 사례 여부: <input type="checkbox"/> 예 <input type="checkbox"/> 아니오 보고 구분 <input type="checkbox"/> 자발보고 <input type="checkbox"/> 조사연구 <input type="checkbox"/> 문헌 <input type="checkbox"/> 모름 <input type="checkbox"/> 기타(_____)		<input type="checkbox"/> 사망 -사망일 ____년 ____월 ____일 -사망 원인 _____ -부검여부: <input type="checkbox"/> 예 <input type="checkbox"/> 아니오 <input type="checkbox"/> 모름 -부검시 입증된 사망 원인 _____ <input type="checkbox"/> 입원 또는 입원기간 연장 <input type="checkbox"/> 선천적 기형 초래 <input type="checkbox"/> 생명의 위협 <input type="checkbox"/> 중대한 불구나 기능적하 <input type="checkbox"/> 기타 의학적으로 중요한 상황 _____			
*조사연구의 경우(계획서 번호/제목: _____) <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> 1) <input type="checkbox"/>개심사 보고 -사후생검적조사 -시판후 임상연구 -특별조사 </div> <div style="width: 45%;"> 2) <input type="checkbox"/>안전성정보조사계획서에 의한 연구 3) <input type="checkbox"/>임상연구 4) <input type="checkbox"/>개별사례연구 5) <input type="checkbox"/>기타(_____) </div> </div>					
*문헌의 경우 (서지정보: _____)					
보고자나 원보고자가 이 사례를 아래의 기관에도 보고하였다면 아는 대로 모두 표시해 주세요. <input type="checkbox"/> 제조·수입회사 <input type="checkbox"/> 지역약물감시센터 <input type="checkbox"/> 한국의약품안전관리원 <input type="checkbox"/> 의료기관 <input type="checkbox"/> 보건소 <input type="checkbox"/> 약국 <input type="checkbox"/> 기타(_____)					
환자 정보 *					
성별: <input type="checkbox"/> 남 <input type="checkbox"/> 여 <input type="checkbox"/> 모름 이름: _____ (예: 홍길동 → 홍ㄱㅇ 또는 HKD) 체중: _____ kg		연령 정보 생년월일: ____년 ____월 ____일 발생당시 나이: ____세 * 정확한 연령 정보가 없는 경우 아래에 표시해 주세요. <input type="checkbox"/> 출생일~28일 미만 <input type="checkbox"/> 28일~24개월 미만 <input type="checkbox"/> 24개월~12세 미만 <input type="checkbox"/> 12세~19세 미만 <input type="checkbox"/> 19세~65세 미만 <input type="checkbox"/> 65세 이상			
부모 정보 ^(환자가 태어나 유아인 경우) :					
임신기간	부모이름	부모성별	부모나이		
_____주	(예: 홍길동 → 홍ㄱㅇ 또는 HKD)	<input type="checkbox"/> 남 <input type="checkbox"/> 여 <input type="checkbox"/> 모름	_____세		
환자 병력 / 약물 사용력 등 상세내용 ^(*) : (환자가 태어나 유아인 경우 부모의 정보 기재)					
질환명 또는 제품명 / 발현증상	시작일	종료일	현재진행여부	상세내용	
유해사례 정보					
유해사례명 *	증상발현일	증상종료일	증상지속기간	강조 ⁽¹¹⁾	중대성 ⁽¹²⁾

특히 위 서식의 [작성시 참고사항]란에서는 “(8) 이름은 개인 식별이 불가능한 형태로 기입하시면 됩니다. (예: 홍길동→홍ㄱㅇ, HKD 등)”이라고 설명하고 있다. 결국 위 보고서 서식은 ‘머리글자로 표시되는 이름, 생년월일, 성별’은 개인 식별이 불가능한 것이라고 판단한 것이다. 이는 의약품의 안전에 관한 주무부처인 식품의

약품안전처의 명시적인 결정이다.

요컨대, 본 사안의 정보는 그 정보에 포함된 생년월일, 성별 등 다른 요소정보들을 종합적으로 고려하더라도 그 자체로는 개인을 식별할 수 없는 것으로 보인다.

(4) 마지막으로, 「개인정보 보호법」은 또 다른 개인식별성의 판단방법으로 “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것”(제2조 제1호 괄호 부분)을 제시하고 있다. 여기서 ‘다른 정보와 쉽게 결합하여’의 의미가 확정되어야 할 것이다.

이 의미를 확정함에 있어서는 앞에서 서술한 비교법적 분석이 참고가 될 수 있을 것으로 보인다. 먼저, 미국의 의료정보보호법(HIPAA)은 ‘개인을 식별할 수 있는 의료정보’의 개념규정에서 식별가능성(identifiability)의 판단 기준으로 ‘그 정보가 개인의 식별에 사용될 수 있다고 믿을 만한 합리적인 근거가 있을 것’(there is a reasonable basis to believe that the information can be used to identify the individual)을 제시하고 있다.³²⁾ 즉, 식별가능성은 판단의 대상이 되는 ‘그 정보’를 기준으로 해서 ‘그 정보’가 개인 식별에 사용될 수 있다고 믿을 만한 ‘합리적 근거’가 있는지를 판단 기준으로 하고 있다. 이는 곧 정보처리자가 ‘합리적으로 접근할 수 있는 다른 정보’와 결합해서 그 정보가 개인 식별에 사용될 수 있는지를 의미하는 것으로 이해된다.

이처럼 식별가능성을 판단함에 있어서 활용될 수 있는 ‘다른 정보’란 그 정보를 처리하는 ‘정보처리자의 입장’에서 접근할 수 있는 정보를 의미한다고 할 것이다. 이 점에 관해서는 영국의 개인정보 보호법도 동일하다. 즉, 영국의 법률은 명시적으로 ‘그 정보’ 외에 ‘정보처리자’(data controller)가 보유하고 있거나(is in the possession) 또는 보유하게 될 것 같은(is likely to come into the possession) 다른 정보를 결합해서 개인이 식별될 수 있는지를 판단하도록 하고 있다.³³⁾ 여기서 ‘보유하게 될 것 같은’이란 ‘통상적으로 쉽게 입수할 수 있는 것’이라고 이해된다. 이는 곧 미국법의 ‘합리적인 근거’(reasonable basis)와 같은 개념이다.

미국과 영국의 이 같은 개념인식을 일본의 개인정보보호법에서는 더욱 분명한 언어로 표현하고 있다. 일본의 법률은 “다른 정보와 용이하게 조합(照合)[서로 맞추어 봄]할 수 있고, 그로써 특정의 개인을 식별할 수 있게 되는 것을 포함한다.”고

32) 앞의 [Ⅲ. 2. (2)] 참조.

33) 앞의 [Ⅲ. 2. (4)] 참조.

규정하고 있다. 즉, 조합(照合)이 ‘용이할 것’을 규정하고 있는 것이다. 실제로 2014년의 「개인정보보호법에 대한 경제산업 분야를 대상으로 한 가이드라인」(후생노동성·경제산업성 고시 제4호)은 이 점을 예를 들어 설명하고 있다. 즉, “다른 정보와 용이하게 조합(照合)할 수 있는”이라 함은 “예를 들어 통상의 작업범위에서 개인정보데이터베이스에 접근해서 조합(照合)할 수 있는 상태를 말하며, 다른 사업자에게 조회(照會)·물어서 알아봄·해야 하는 경우 또는 당해 사업자 내부에서도 취급 부문이 다른 경우 등 조합(照合)이 곤란한 상태를 제외한다.”고 명확하게 해설하고 있다.³⁴⁾

마찬가지로 한국의 「개인정보 보호법」도 동일한 국제적 흐름을 따라서 “다른 정보와 쉽게 결합하여 알아볼 수 있는 것”을 포함한다고 규정하고 있다. 따라서 ‘다른 정보와 쉽게 결합하여’의 의미는 ‘정보처리자가 통상적인 업무과정에서 쉽게 입수할 수 있는 다른 정보와 결합하여’의 의미로 해석되어야 마땅할 것이다. 이 같은 해석론은 위 비교법적 논거 외에도 문리적·논리적 해석의 관점에서도 타당한 것으로 보인다. ‘쉽게 결합하여’는 ‘결합이 쉽다’는 뜻이고, 쉽게 입수할 수 없는 것은 결합이 어려운 것임은 논리적으로 당연하다.

더 나아가, 한국의 「개인정보 보호법」은 외국의 그것과 비교해서 지나치게 과도한 형사처벌규정을 두고 있다는 점을 고려하여야 한다. 「형법」처럼 봉합된 사생활 비밀을 보호하는 것이 아니라, 공개된 개인정보까지도 포함하여 매우 광범위한 개인정보(개인에 관한 일체의 정보)에 관해 그 보호와 이용의 가치를 균형 있게 조정하는 법제에서, 그것도 구체적인 법익침해에 대한 사후입법이 아닌 사전규제의 위협예방법에서, 이렇게 과도한 형사처벌규정을 두고 있는 외국의 입법례는 실로 찾아보기 어렵다.

일본의 개인정보보호법만 하더라도 규율대상자인 정보처리자(‘個人情報取扱事業者’)는 ‘개인정보데이터베이스를 사업(事業)에 이용하는 자’에 한정되고(한국은 ‘업무를 목적으로 개인정보파일을 운용하는 자’), 정보처리자가 법률이 정한 처리기준과 의무를 위반한 경우 바로 형사처벌을 가하는 것이 아니라, 행정청(主務大臣)이 1차로 시정권고를 하고 2차로 ‘개인의 중대한 권리이익의 침해가 임박했다고 인정하는 경우’에 시정명령을 내리며, 그래도 이행하지 않는 경우 6월 이하의 징역 또는 30만엔 이하의 벌금에 처하고 있다(제34조 및 제56조).

그러나 한국의 법률은 애매한 처리기준에 더하여 과도한 형사처벌규정이 많다.

34) 앞의 [Ⅲ. 2. (5)] 참조.

이 사안의 정보만 하더라도 만일 식별가능성이 인정되는 개인정보라고 한다면, ‘건강정보’로서 법 제23조의 ‘민감정보’에 해당하여 정보주체의 사전 동의를 받거나 법령이 처리를 허용하는 경우 외에는 그 처리(수집·이용·제공)에 대해 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해지게 된다(법 제71조 제3호). 이러한 형사처벌의 적용대상 여부를 판가름하게 되는 ‘개인정보’의 해당 여부 및 식별가능성 판단기준을 해석함에 있어서는 헌법 제12조의 죄형법정주의에 따른 엄격해석이 요구되고 함부로 확장해석을 해서는 안 될 것이다. 合憲的 法律解釋은 법률을 집행하거나 적용하는 모든 국가기관에 요구되는 법률해석의 원칙이다.

이상을 정리하면, 「개인정보 보호법」 제2조 제1호 괄호 부분의 “다른 정보와 쉽게 결합하여”란 ‘정보처리자가 통상적인 업무과정에서 쉽게 입수할 수 있는 다른 정보와 결합하여’의 의미로 해석되어야 마땅할 것이다. 그리하여 위 일본의 해석론처럼 ‘다른 사업자에게 조회(照會)[물어서 알아봄]해야 하는 경우’나 ‘통상적인 업무과정에서 입수하는 것이 곤란한 경우’는 제외되어야 한다.

(5) 이상의 해석론으로 본다면, 2011년의 ‘증권통 앱 사건’의 판결³⁵⁾은 아쉬움이 큰 무리한 확장해석 및 적용이라고 평가될 수 있다. 이 판결은 법 제2조 제1호 괄호 부분의 ‘쉽게 결합하여 알아볼 수 있다’는 문언의 의미를 지나치게 확장하여, “쉽게 다른 정보를 구한다는 의미이기보다는 구하기 쉬운지 어려운지와는 상관없이 해당정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다.”고 해석하고 있다. 그러면서 판결은, 휴대폰에 부여되는 기기 고유번호인 IMEI와 USIM 카드의 일련번호는 그 자체로는 개인을 알아볼 수 없는 정보라는 점을 인정하면서도, 이동통신사의 고객관리DB 안에서 이들 일련번호와 그 사용자의 신원확인정보(이름, 주민등록번호)가 결합되어 관리되고 있다는 점을 들어, 이들 번호가 개인을 알아볼 수 있는 정보라고 판단하였다.

그러나 이들 기기 고유번호만을 수집한 증권통 앱 운영자가 이동통신사의 고객관리DB에 접근하는 것은 법적으로 허용되지 않고 현실적으로도 거의 불가능하다(고도의 해킹기술을 통해서만 가능). 판결에서도 “IMEI나 USIM 일련번호와 관련된 개인에 관한 정보는 각 통신사별로 그 접근에 엄격한 통제를 가하고 있다.”는 사실인정을 분명히 밝히고 있다. 그렇다면, 이들 번호를 수집한 정보처리자(앱 운영자)가 그 앱을 통해 수집하는 다른 정보와의 결합을 통해 그 정보주체를 알아볼

35) 서울중앙지방법원 2011. 2. 23. 선고 2010고단5343 판결.

수 있는지를 평가하는 것은 충분히 가능하고 타당한 접근방식이지만, 앱 운영자가 법적으로나 사실적으로 접근이 거의 불가능한 다른 사업자(이동통신사)의 고객관리DB에 이들 기기번호와 신원확인정보가 결합되어 관리되고 있다는 점을 주된 논거로 삼는 것은 타당하지 못한 접근방식이 아니었는가 하는 생각이다.

구태언 변호사도 위 판결의 부당성을 다음과 같이 매우 적절하게 지적하고 있다. 즉 “사실상 결합될 가능성이 없는 정보가 추상적으로 쉽게 결합될 수 있다는 이유만으로 ‘개인정보성’을 가지게 되고, 그로 인하여 형사처벌을 받게 되는 경우가 발생할 수 있다. 이와 같은 논리라면 부진정 개인정보는 어디엔가 보관되어 있을 진정 개인정보와의 결합가능성 때문에 언제나 법상 개인정보가 된다는 부당한 결론에 이르게 된다.”³⁶⁾

결국 서울중앙지방법원의 위와 같은 확장적인 해석·적용은 문리적·논리적 해석의 관점에서 보거나 죄형법정주의의 엄격해석의 원칙에 비추어 타당하지 않으며, 일본과의 비교법적 관점에서도 지나친 것이라고 판단된다.

V. 결론

본 사안의 정보가 ‘다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는지’ 여부는 정보를 제공받은 민간의 기업이 ❶ 통상의 업무과정에서 약국의 처방전DB나 병·의원의 환자정보DB에 쉽게 접근할 수 있는지 여부 및 ❷ 그밖에 일반인이 접근할 수 있는, 환자정보가 담긴 공공의 데이터베이스가 존재하고 또 그것에 쉽게 접근할 수 있는지 여부에 관한 사실인정 여하에 달려 있다고 하겠다. 위 사실문제를 판단할 수 있는 입장에 있지는 않지만, 접근이 매우 어렵거나 불가능할 것으로 보인다. 왜냐하면 통상적으로 신원확인정보가 담긴 환자정보데이터베이스에 접근한다는 것 자체가 규범적으로 형사처벌을 수반하는 범죄행위가 될 것이기 때문이다.

법은 **善과 衡平**의 기술이다. 사회적으로 상충하는 가치와 이익들을 균형 있게 조정하지 못한다면 궁극적으로 사회적 **善**도 달성하지 못하게 된다. 로마법대전의 이 격언은 시간을 뛰어넘어 현재 한국의 「개인정보 보호법」을 해석·적용함에 있어서 반드시 유념해야 할 교훈이다. 안전하게 익명화된 처방전 정보를 제한적인 정보공유를 통해 연구나 통계분석 등의 목적으로 활용하는 것을 ‘특정의 누군가’에

36) 구태언, 개인정보 정의조항, 동의제도 및 형사처벌의 합리화에 관한 연구, 고려대학교 정보보호대학원 석사학위논문, 2013, 98면.

관한 정보라는 이유만으로 죄악시하거나 불법화하는 것은 법으로서의 균형을 잃은 것이다.

* 논문최초투고일: 2015년 3월 31 일; 논문심사(수정)일: 2015년 4월 17일; 논문게재확정일: 2015년 4월 24일

[별지 1] 증례기록서 예시

Protocol No.: YCD173
YHD1044 Phase I MAD + 2
CRF ver.02



증례기록서 (Case Report Form)

조루 남성 지원자를 대상으로 YHD1044 반복경구투여 시
안전성, 내약성, 약동학적 특성 및 유효성 평가를 위한 용량군별 무작위배
정, 이중눈가림, 위약/활성대조, 반복투여, 단계적 증량 제 1/2 상 임상시험

A dose-block randomized, double-blind, placebo/active-controlled, multiple dosing,
dose-escalation phase I / II clinical trial to investigate the safety, tolerability,
pharmacokinetics and efficacy of YHD1044 after oral administration in premature
ejaculation patients

연구자 정보	실시기관 [Investigating Institute] :	
	시험책임자 [Principal Investigator]	

피험자 정보	스크리닝 번호 [Screening No.]	
	배정번호 [Enrollment No.]	
	피험자 이니셜 [Initials]	

CONFIDENTIAL

본 임상시험과 관련된 모든 정보는 기밀사항이며 ㈜유한양행의 독점소유자산이므로 ㈜유한양행의 사전
서면 동의 없이는 정보를 유출할 수 없습니다.

Protocol No.: YCD173
YHD1044 Phase I MAD + 2
CRF ver.02



유신양행

PAGE

3

VISIT 1 Day-35 ~ -1	방문일 [Visit Date]	피험자이니셜 [Initial]	스크리닝번호 [No.]
	<div style="display: flex; justify-content: space-around;"> <div>Y</div><div>Y</div><div>M</div><div>M</div><div>D</div><div>D</div> </div>	<div style="display: flex; justify-content: space-around;"> <div></div><div></div><div></div> </div>	S - <div style="display: flex; justify-content: space-around;"> <div></div><div></div><div></div> </div>

피험자 동의 [Informed Consent]		IC
동의취득일 [Date]: _____ yy/mm/dd ▶ 피험자 동의가 이루어지지 않았다면, 본 임상시험에 참여할 수 없음. ☞ 제외 ▶ 임상시험 시작을 위해 가장 먼저 수행되어야 하며, 동의일자는 동의서 원본과 동일하여야 함.		
인구학적 정보 [Demographic Data - Screening]		DD
생년월일: _____ yy/mm/dd 연령(만): _____ 세 ▶ (동의년도)-(출생년도)= OO 세 (동의일 기준 생일이 지나지 않은 경우 -1 세) ▶ 만 19 세 이하 65 세 이상 ☞ 본시험에서 제외 체중: _____ kg 키: _____ cm BMI: _____ ▶ 50kg 미만~90kg 초과 ☞ 제외 ▶ BMI = 체중(kg)/(신장(m)) ² ▶ 18 미만 27 초과 ☞ 제외		
이전 임상시험 참여여부:	<input type="checkbox"/> 예 [Yes] _____ yy/mm/dd	<input type="checkbox"/> 아니오 [No]
전혈 공여 여부	<input type="checkbox"/> 예 [Yes] _____ yy/mm/dd	<input type="checkbox"/> 아니오 [No]
성분헌혈 공여 여부	<input type="checkbox"/> 예 [Yes] _____ yy/mm/dd	<input type="checkbox"/> 아니오 [No]
수혈 여부	<input type="checkbox"/> 예 [Yes] _____ yy/mm/dd	<input type="checkbox"/> 아니오 [No]
흡연 [Smoke_ciga]: <input type="checkbox"/> 현재 <input type="checkbox"/> 과거(1 개월 이전) <input type="checkbox"/> 피운 적이 없다 담배 [Cigarettes] _____ 개피/일 ▶ 하루 담배 10 개피 이상 ☞ 본시험에서 제외 음주 [Alcohol]: <input type="checkbox"/> 현재 <input type="checkbox"/> 과거(1 개월 이전) <input type="checkbox"/> 마신 적이 없다 음주량 _____ g/일 * 섭취한 알코올의 양(g) = 섭취량(ml) x 도수(%) x 0.8 소주(20%), 맥주(5%), 막걸리(6%), 포도주(12%), 양주(40%) ▶ 음주량 30g/day 초과인 경우 ☞ 본시험에서 제외 카페인 [Caffeine]: <input type="checkbox"/> 예 [Yes] <input type="checkbox"/> 아니오 [No] 커피, 차 _____ 컵 (250cc)/일 ▶ 카페인 5 컵/day 초과인 경우 ☞ 본시험에서 제외 콜라 [Coke] _____ 컵 (200cc)/일 비정상적 식이 <input type="checkbox"/> 예 [Yes] ▶ _____ (자몽 포함) <input type="checkbox"/> 아니오 [No]		

Abstract

There is a set of medical prescription data which indicates that an orthopedic surgeon at the Jinhae Yonsei Clinic prescribed five day doses of ALBIS TAB made by the Daewoong Pharm for a woman born in August 30th, 1966 whose resident registration number was encrypted. Do the anonymized prescription data fall under the category of ‘personal data’ under the Personal Data Protection Act of Korea? Or not?

It is apparent that the data is about some particular person. But the problem is whether she can be identified from the data or other information which is in the possession of, or is likely to come into the possession of, the data controller. Under the Act of Korea, the term “personal data” means “information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified, (including information by which the individual in question cannot be identified but can be identified through simple combination with other information).”

The main issue of this paper is whether a particular woman as the above data subject can be identified by the encrypted resident registration number, date of birth and sex. It concludes that an encrypted resident registration number which can not be deciphered, birth date, and sex themselves can not be used as personal identifiers. In its final analysis, the above anonymized prescription data fall out of the category of ‘personal data’ under the Act.

Keywords: Personal Data Protection Act of Korea (PDPA), personal data, personally identifiable information, data anonymity, de-identification, personal identifier, medical prescription data

