

개인정보의 적절한 활용 관련 법적 연구*

—건강정보의 상업적 활용등 이슈를 중심으로—

Legal Issues Related to Proper Process of Personal Information

—Focused on Some Issues about Commercial Use of
Health Information—

양 기 진**

GiJin Yang

목 차

- | | |
|------------------------|----------------------------|
| I. 서론 | III. 적절한 정보 활용 지원을 위한 법적 개 |
| II. 개인정보 활용 관련 규제 현황 및 | 선 방향 |
| 문제점 | IV. 결론 |

현행 개인정보 법제는 개인정보의 신용정보 여부에 따라 소관법과 소관당국을 달리하는데 이러한 방식은 법규 준수를 어렵게 하고 불확실성을 초래한다. 특히 현행 신용정보법은 상거래 정보를 신용정보로 명시적으로 포섭하고 있고 이에 따라 종래 잠재되어 있던 신용정보와 개인정보의 간섭에 관한 논의를 불가피하게 만들고 있다. 개인정보 보호에 관하여 일반법인 개인정보법이 있는 이상, 개인정보 보호에 관한 사항은 개인정보법에 통합시키고 개인정보위원회에 권한을 주고 신용정보법은 신용정보회사 등에 관한 감독법으로 정체를 개편·확립하여야 할 것이다.

두 번째로는 민감정보인 건강정보의 활용·제공 이슈가 있다. 의료법 등 관련법의 제동

<https://doi.org/10.35148/ilsilr.2021..48.673>

투고일: 2021. 1. 31. / 심사회의일: 2021. 2. 4. / 게재확정일: 2021. 2. 15.

* 본 연구결과는 2020년 12월 (주)하나은행 하나금융경영연구소의 후원을 받아 수행되었으며, 2021년 2월 5일 경제학공동학술대회에서 발표되었던 것을 수정·보완하였습니다.

** 전북대학교 법학전문대학원 교수

Professor, School of Law, Jeonbuk National University

에 불구하고 건강정보를 어느 수준에서 어떠한 절차를 거쳐 허용할지 관장하는 법이 마련되어 있지 않다. 이러한 법적 불확실성은 입법에 의하여 해결되어야 한다.

세 번째로, 정보주체의 동의 없이 개인정보의 활용을 가능하게 하는 과학적·산업적 연구 목적의 범위에 대해서 충분한 공론화를 통하여 적절한 입법을 할 필요가 있다. EU 개인정보 보호 일반규정(General Data Protection Regulation) 및 근래 2020년 1월 EU데이터 보호 감독자(European Data Protection Supervisor)가 공개한 해석, 그리고 근래 캘리포니아 소비자 프라이버시법(California Consumer Privacy Act)의 동향을 참조하면, ‘과학적 연구’ 목적으로 개인정보 처리를 허용하기 위하여는 공익 내지 공공성 요건을 요구하는 것이 타당하다.

네 번째로 추가처리에 관한 해석이다. 추가처리 허용규정은 결국 정보처리자와 정보주체의 편의성을 함께 고려하고자 도입된 규정이므로, 정보주체의 기대가능성을 고려하여 균형잡힌 입법이 필요하다. 현행 신용정보법과 같이 추가처리를 널리 가능하도록 하는 입법은 개인의 자기정보 결정권을 해할 가능성이 적지 않으므로 입법적 시정이 필요하다.

[주제어] 개인정보, 신용정보, 건강정보, 의료정보, 추가처리, 과학적 연구 목적

I. 서론

2020년 1월 개인정보 보호법 등 개인정보 관련 3개의 법률(소위 ‘데이터 3법’) 개정안이 국회에서 일괄 가결되어 2020년 8월 5일 시행되었다. 이로 인하여 「개인정보 보호법」(이하 ‘개인정보법’), 「신용정보의 보호 및 이용에 관한 법률」(이하 ‘신용정보법’)이 대폭 개정되고 종래 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 ‘정보통신망법’)상 개인정보 보호에 관한 내용은 개인정보법으로 일괄 이관되었다.

이러한 데이터 3법의 개정 배경에는 다양한 요인이 존재하겠으나 주된 이유로는 기술 개발과 데이터기업의 급성장에 따른 데이터가치의 재인식, 이에 따른 개인정보의 산업적 활용 기반을 마련하여 데이터산업을 육성하면서도, 개인정보의 실효적 보호 제고의 필요성 등을 거론할 수 있을 것이다.¹⁾ 이에 더하여 개인정보 수집·제공 동의의 형식화로 인한 개인정보주체들의 불만과 함께 개인정보 침해행위가 다수 발생하면서도 이를 사전에 효과적으로 막지 못하는 법제에 대한 비판도 누적된 상황이었다. 또한 유럽연합

1) 4차 산업혁명 시대가 도래하면서 발달된 빅데이터 처리기술에 의한 정보주체의 식별 여지가 커짐에 따라 기술 환경 변화에 따른 적절한 대처가 필요하고, 정보 시장 내의 정보 비대칭성이 존재하는 상황에서 정보의 유통마저 원활하지 않아 소수 회사들의 정보 독점 비대 현상도 해결될 필요도 있었음을 들 수 있다. 예컨대 정 전 개인정보 관련법에는 엄격한 정보수집 사전 동의를 요하는 체계에서 원수집 목적의 추가 처리 개념이 부재하였고 가명처리나 가명정보에 관한 합리적인 지위를 부여하는 내용이 없었다.

(EU)에서 2016년 4월 채택되어 2018.5.25.부터 시행된 EU 개인정보 보호 일반규정 (General Data Protection Regulation, 이하 ‘GDPR’)에 의하여 EU 거주민 개인정보의 국내 이전에 관한 EU 측의 적정성 승인을 획득하고자, EU 측의 승인거부 이유로 알려진 개인정보 각법의 관할부처별로 쪼개진 정보감독권한을 집중시키고 관할 부서의 독립성을 제고하는 것이 필요하였다.

이 글에서는 근래 대폭 개정된 데이터 3법에 의하여 개인정보의 원활한 활용에 지장이 없을지의 이슈에 관하여, 최근 잠재적인 이용가치로 주목되는 건강정보 결합을 중심으로 검토하고 시사점을 제시하고자 한다.

II. 개인정보 활용 관련 규제 현황 및 문제점

1. 개인정보 결합 규제

이 글에서는 주로 현행법상 개인정보 활용이 얼마나 자유로울 수 있는지와 관련하여 개인정보의 결합을 관장하는 개인정보법과 신용정보법을 위주로 검토한다. 신용정보집합물 간 결합근거나 비신용 개인정보집합물 간 결합근거는 각 법상 비교적 명백한 반면 (신용정보법 제17조의2, 개인정보법 제28조의3 등), 개인정보집합물과 신용정보집합물 간의 결합에 대해서는 양법 모두 적용될 소지가 있는데 명시적인 규정이 없으므로 법적 불확실성이 존재한다.

이하에서는 개인정보집합물과 신용정보집합물을 결합함에 있어서 현행 개인정보법과 신용정보법을 검토하여 원활한 데이터 결합·활용에 법제상 장애가 되는 측면이 있는지 살펴보고, 데이터활용과 개인정보주체(겸 소비자) 보호 필요성을 조화하기 위하여 EU의 GDPR 및 2018년 제정·2020년 1월 시행된 미국의 캘리포니아 소비자 프라이버시법 (California Consumer Privacy Act)을 참고하여 향후 법제 개선방향을 제안하고자 한다.

2. 개인정보 범위의 해석상 축소 및 관련 문제

개정 개인정보법 및 신용정보법은 모두 가명정보를 법의 보호대상으로 한다. 개인정보법은 개인정보의 범위에 대하여 생존하는 개인에 대하여 “개인을 알아볼 수 있는

정보”(개인직접식별정보)와 함께 “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보”(개인식별가능정보)도 개인정보도 본다(법 제2조제1호 나목 전단). 나아가 개인정보법은 가명정보를 동법상 개인정보의 유형으로 추가적으로 정의하고 ‘가명정보’를 이상의 개인직접식별정보나 개인식별가능정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보”(추가정보에 의한 개인식별가능정보)로 정의한다(법 제1조 제1호 다목). 또한 이 때의 ‘가명처리’란 추가정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것으로 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법을 들 수 있다(법 제1조 제1호의2).

반면, 신용정보법상 ‘개인신용정보’란 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보여야 함을 전제로, 특정 개인을 알아볼 수 있는 정보(개인직접식별정보) 또는 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보(개인식별가능정보)를 말한다(법 제2조 제2호). 또한 신용정보법은 ‘가명정보’를 가명처리한 개인신용정보로 하고 ‘가명처리’에 대해서도 개인정보법과 별도로 정의를 두고 있다. 동법상 ‘가명처리’란 “추가정보를 사용하지 아니하고는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리”하는 것으로 정의되며 이 경우 그 처리결과가 (i) 어떤 신용정보주체와 다른 신용정보주체가 구별되거나, (ii) 하나의 정보집합물²⁾에서 또는 서로 다른 복수의 정보집합물 간에서 어떤 신용정보주체에 관한 둘 이상의 정보가 연계·연동되는 경우 등을 말한다(법 제2조제15호).

개인정보법이나 신용정보법 모두 ‘식별가능성’이 있는 경우 법의 보호대상인 개인(신용)정보로 하고 있기때문에 식별가능성에 관한 판단기준이 문제된다. 개인정보법은 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는지 여부를 판단함에 있어서 고려할 사항을 규정하면서도(법 제2조제1호 나목 후단³⁾) 누구의 관점에서 식별가능성을 판단할지 명시적 규정은 두지 않고 있으며, 신용정보법은 따로 규정을 두고 있지 아니하다.

어느 누구의 관점에서 식별가능성의 존부를 판단할 것인지 논란이 있는 상황에서, 개인정보보호위원회(이하 ‘개정위’)는 2020년 9월 「가명정보 처리 가이드라인」을 제정

2) 통상 데이터베이스를 지칭한다.

3) “쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는시간, 비용, 기술 등을 합리적으로 고려하여야 한다”(개인정보법 제2조제1호 나목 후단).

하였고 동 가이드라인은 종전에 행정안전부의 주관으로 2016년 6월 제정된 「개인정보 비식별 조치 가이드라인」의 입장을 좇아 상대설의 입장을 채택하고 있다. 개정위의 가명 정보 처리 가이드라인은 개인정보에 대한 판단기준에 관하여 ‘가명정보처리자’의 관점에서 처리자가 보유하는 정보 또는 접근가능한 권한 등 상황에 따라 판단하며, 가명정보 처리자가 보유한 다른 정보 등을 통해 개인 식별이 가능한 경우 가명처리가 잘못된 경우라고 하는 등⁴⁾ 명백히 ‘상대설’을 취한다.⁵⁾

이러한 입장은 EU GDPR과 사뭇 다르다. GDPR은 정보처리자의 관점은 물론, 타인의 관점을 함께 고려하여 식별가능성 존부, 즉 보호대상인 개인정보 성 해당 여부를 결정하는 ‘절충설’을 취하고 있다. GDPR은 식별가능성의 판단에 해당 정보처리자는 물론 ‘타인’ 역시 사용할 수 있다고 합리적으로 여겨지는 가능한 모든 수단을 고려하도록 하며 이 때 ‘합리적으로 사용 가능한 수단’의 판단에는 정보 처리당시 입수가 가능한 기술 및 기술발전을 감안하여 식별에 요구되는 모든 객관적 요소(소요비용 및 시간 등)를 고려하도록 하고 있다(GDPR Recital 26.). GDPR이 채택한 절충설 하에서는 구체적 상황에 따라 개인정보로 판단될 여지가 상대설에 비하여 더 많아질 수 있음에도, 합리적인 인간의 관점에서 사회적으로 납득가능한 보다 객관적·일관된 기준을 제시하는 것이 가능하다.

3. 개인정보 중 신용정보와 비 신용정보 간의 결합

3.1 신용정보법과 개인정보법의 관계

개인정보법은 개인정보 보호에 관한 일반법으로⁶⁾ 신용정보법은 법체계상 개인정보법의 특별법이라고 할 수 있다. 따라서 신용정보에 해당하는 정보와 그렇지 아니한 비신용 개인정보를 함께 처리할 때에는 두 법을 따라야 한다. 그런데 현행 신용정보법은

4) 개인정보보호위원회, 「가명정보 처리 가이드라인」, (2020.9.), 7~9쪽, <<https://www.pipc.go.kr/np/default/page.do?mCode=D040010000#LIN>>

5) 그러나 상대설의 채택은 바람직하지 않다. 개인정보 성 여부의 판단을 ‘해당 정보를 처리하는 자의 관점’에서 처리하는 상대설은 식별가능성 존부 관련 조사를 정보처리자의 잘 알려진 반경(well-known sphere of the controller)에 한정하는데, 이처럼 정보처리자의 반경만을 고려한다면 개인정보에 해당하는 범위가 합리적인 사람의 관점에서 볼 때 납득이 어려울 정도로 제약될 수 있다. 양기진, “개인정보의 범위에 관한 연구- GDPR의 비식별조치와 약학정보원 사건의 검토”, 선진상사법률연구 통권 제84호, 법무부, (2018.10.), 64쪽.

6) 개인정보 법은 다른 법률과의 관계에 대하여 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다(법 제6조)

신용정보업자에 대한 감독에 관한 사항을 차치하고 개인정보 보호·처리에 대하여 개인정보법의 특별법적 지위를 벗어나 소관부서는 물론, 규율대상인 신용정보 등 기본 개념에 대해 별도로 규정하고 개인정보법과 상당부분 다른 내용을 규율함으로써 일반법인 개인정보법의 규율 내용과 상당부분 유리되어 있다. 현행 법제상 두 법은 서로 다른 당국이 소관하는 별개의 법으로 볼 수 있을 정도로 독립적이나 개인정보를 다룬다는 점에서 양법은 밀접히 관련된다.

개인신용정보가 되기 위하여는 선결문제로 ‘신용정보’에 해당하여야 한다. 신용정보법상 ‘신용정보’는 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보로서 (i) 특정 신용정보주체를 식별할 수 있는 정보, (ii) 신용정보주체의 거래내용을 판단할 수 있는 정보, (iii) 신용정보주체의 신용도를 판단할 수 있는 정보, (iv) 신용정보주체의 신용거래능력을 판단할 수 있는 정보, 그 외에 이상의 정보 외에 (v) 신용정보주체의 신용을 판단할 때 필요한 정보를 말한다(신용정보법 제2조제1의2호 내지 제1의6호 및 영 제2조제17항).

개정 신용정보법은 신용정보의 개념을 법률로 끌어올려 규정하면서도 상법상 상행위에 따른 상거래 정보를 신용정보로 포함시키는 등 신용정보의 외연을 크게 넓혔다. 상법상 상행위는 영업을 위하여 행하는 직·간접적인 일상적 거래행위를 모두 포괄하는 광범위한 개념이다. 따라서 현행 신용정보법상 개인신용정보의 범주가 크게 확대되면서 개인정보법의 적용대상인 비신용 개인정보와의 구분이 많은 경우 곤란하여졌다.

3.2 입법에 의한 개인신용정보의 확대와 파생 문제점

금융회사라면 개인신용정보든 비신용 개인정보든 상관없이 소비자에게 가장 적절한 금융상품을 설계하여 맞춤형 판매를 하는데에 관심이 많을 것이다. 예컨대 보험업계의 경우 맞춤형 보험상품 설계·판매를 하고자 할 유인이 클 것인데, 이를 위해서는 비신용 개인정보인 건강정보를 함께 활용할 요구가 커진다.

이러한 상황에서 건강정보를 금융정보를 가명처리하여 정보주체의 동의 없는 [산업적] 연구목적, [상업적] 통계작성 목적으로 이용하는 것이 가능할까. 건강정보는 그 자체로는 일반적으로 신용도 판단과 상관없으므로 개인정보법이 적용되는 비신용 개인정보라고 할 것이다. 또한 건강정보는 개인정보법상 대표적인 민감정보⁷⁾에 해당한다. 개인정

7) 개인정보법은 민감정보를 “사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에

보법은 민감정보의 처리는 허용하면서도 민감정보의 성격상 ① 정보주체의 별도 동의 또는 ② 법령상 근거가 주어지는 경우에 예외적으로 처리를 허용한다(개인정보법 제23조제1항).

그런데 개인정보법은 가명정보의 처리와 관련하여 “통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이” 가명정보를 처리할 수 있음을 규정한다(개인정보법 제28조의2 제1항). 개인정보법 제28조의2 제1항에는 적용대상에서 민감정보를 배제하고 있지 아니하다. 따라서 건강정보와 같은 민감정보라도 일반적으로 개인정보법 상 과학적 연구 등 목적을 위하여 정보주체의 동의 없이 처리가 가능한지 논란⁸⁾이 가능하다.

두 번째로 개인정보법 제28조의2 제1항은 “통계작성, 과학적 연구, 공익적 기록보존 등”을 위한 가명정보 처리를 허용하나 신용정보법(제32조제6항 제9의2호)과 달리 산업적 연구나 상업적 통계 목적으로 확대하고 있지는 아니하다. 따라서 비신용 개인정보인 건강정보와 신용정보에 해당하는 금융정보를 가명처리한 후 이를 결합하여 산업적 연구나 시장조사 목적의 통계 처리 목적으로 정보처리를 할 수 있는지 의문이 불가피하다. 고령화 심화 추세로 건강 관리 사업의 성장세가 향후 더욱 커질 것으로 전망되는 이상, 비신용 개인정보로서의 건강정보를 산업적 연구 목적으로 이용되려는 수요가 특히 민간 영역을 중심으로 클 것으로 보인다.

4. 건강정보의 처리 허용 범위

4.1 민감정보인 건강정보의 처리 가부

건강정보는 개인정보법 상 민감정보에 해당하면서 의료법 등에 의하여도 특별한 지위를 갖는다. 우선, 건강정보는 대표적인 민감정보로서 개인정보법 상 처리가 제한된다. 다만 제3자에게 제공함이 없이 정보처리자가 가명 처리하는 행위 자체는 정보 자체에 대한 보안성을 높이므로 정보주체의 명시적 동의 없이도 허용될 것이다.⁹⁾ 그러나 건강정

관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보”로 정의한다(개인정보법 제23조제1항).

8) 의료정보를 비롯한 민간정보에 대해서도 가명 처리가 허용될 수 있는지를 둘러싼 논란으로, 전승재, “개인정보, 가명정보 및 마이데이터의 활용 범위-데이터 3법을 중심으로”, 선진상사법률연구 통권 제91호, 법무부 (2020.7.).

보를 타인에게 제공하는 행위는 현행법상 제약이 있다. 우선 의료정보는 의료법상 정보 누설이 금지되어 있으며(의료법 제19조), 환자 외 기록 열람도 엄격히 제한된다(의료법 제21조). 국민건강보험법상으로도 직무상 목적 외 용도로 개인정보를 제3자에게 제공할 수 없다(국민건강보험법 제102조). 이들 법이 엄연히 기능하는 이상 개인정보법이 현행법을 명문으로 뒤집는 해석을 하여 외부 정보누설이나 제3자 정보제공을 허용하는 것은 개인정보법의 문언상으로도 어렵다.¹⁰⁾

그럼에도 불구하고 개인정보법에 따라 건강정보를 원 수집목적 외로 추가처리하거나(법 제28조의2 제1항) 이를 가명처리하여 ‘처리’(제3자 제공등)할 수 있는지(법 제28조의2)에 관하여 건강정보의 처리를 허용하여야 한다는 정부의 해석이 존재함에 따라 처리 관련 논란¹¹⁾이 존재한다.

민감정보인 건강정보의 활용·제공 이슈는 정보누설을 금지하는 의료법에 위반할 소지가 커서 상당한 법적 불확실성이 존재한다. 이 문제는 현행처럼 관련법의 입법이 이뤄진 이후 드러난 사각지대를 가이드라인과 같은 정부의 ‘해석’으로 대응하는 것은 법적 불확실성을 해결하는데 도움이 되지 않는다.¹²⁾ 따라서 문제를 현출시켜 사회적 논의 후 입법적으로 해결하는 것이 필요하다.

4.2 비신용 개인정보 처리 관련 법적 불확실성

건강정보의 추가처리 또는 가명처리 후 과학적 연구 등 활용이 가능한지, 즉 신용정보 등과 결합하여 가치창출이 가능할지 이하에서 검토한다.

4.2.1 건강정보의 추가처리 가부

개정 개인정보법 및 신용정보법상 도입된 소위 ‘추가처리’ 규정에 의하여 건강정보를 정보주체의 동의 없이 이용·제공하거나(개인정보법) 또는 제공하는(신용정보법) 것이

-
- 9) 가명처리를 거칠 경우 개인정보의 보안성이 강화되므로 이는 적절한 추가처리에 해당될 것이다.
- 10) 개인정보법 제6조는 “개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.”고 하여 개인정보법의 보충적 적용을 명시하고 있다.
- 11) 건치신문, “보건의료 데이터 활용 가이드라인 철회!” (2020.9.2.), <<https://www.gunchinews.com/news/articleView.html?idxno=60794>>.
- 12) 가이드라인은 법규 명령이 아니므로 그 내용은 법원을 기속할 수 없다. 아울러 우리 사회에서 관련 논의가 충분히 이뤄지지 않은 상황에서 정부가 일방적으로 이끄는 형국으로 해당 가이드라인의 설득력 역시 매우 미흡하다.

허용될지 의문이 들 수 있다. 우선 비 신용 개인정보의 추가처리와 관련하여, 개인정보법은 개인정보처리자가 정보주체의 동의 없이 개인정보를 이용하거나 제3자 제공하려면 당초의 수집목적과 ‘합리적인 관련성’이 있을 것을 요건으로 개인정보의 이용·제공을 허용한다(법 제15조제3항 및 제17조제4항). 이때 합리적 관련성 여부를 판단하기 위하여 고려하여야 하는 요소에 관하여 (i) 당초 수집 목적과의 관련성, (ii) 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성, (iii) 정보주체 이익의 부당한 침해 여부, (iv) 가명처리 또는 암호화 등 안전성 확보 조치 여부로 정하고 있다(개인정보법 시행령 제14조의2 제1항).

일반적으로 의료인의 경우 환자로부터 진료목적으로 수집동의를 받은 의료정보를 자신 또는 제약회사의 이익추구 목적 임상실험에 제공하는 것은 원 수집목적과의 관련성이 있다고 보기 어려울 것이다. 또한 휴대폰의 건강관리 앱 등을 통하여 취득한 휴대폰 이용자의 건강정보를 기업이 자사 또는 타사의 제품 개발 등 목적으로 이용·제공하는 것 역시 개인정보법 상 추가처리 규정으로는 정당화되기 어려울 것이다.

4.2.2 가명처리 후 과학적 연구 등 목적 처리 가부

건강정보를 가명처리한 후 개인식별에 사용될 수 있는 정보를 삭제한 뒤 해당 가명정보를 개인정보 법에 따라 과학적 연구 등 목적을 위하여 스스로 이용하거나 제3자에 제공할 수 있는지 문제된다(법 제28조의2). 이에 대하여 개인정보 법에서 이를 해결하기 위한 명시적 규정은 두고 있지 아니하다. 그러나 의료법 등 관련 법에서 대표적인 민감정보에 해당하는 의료정보의 제3자 누설 금지 등을 고려한 취지에 의하면 개인정보 법이 민감정보로 별도 규율하는 취지를 위배하여 건강정보에 가명조치를 취할 경우 정보 주체의 동의 없이 이를 처리할 수 있다고 보는 것은 위험한 해석이다.¹³⁾ 개인정보 법은 개인정보 보호에 관하여 타법에 대해 동 법이 보충적으로 적용됨을 명문으로 선언하고 있기도 하다(법 제6조).

다음 단계로 과학적 연구 등 목적을 위하여 개인 건강정보를 가명처리하여 처리하는 것이 허용되더라도 이를 신용정보 집합물과 결합할 경우에는 개인정보 법이 적용될지 또는 신용정보법이 적용될지 이슈가 있게 된다. 산업적 연구나 상업적 통계 목적의 정보

13) 최근 시민단체에서는 연구 등 목적을 위하여 가명처리 된 질병정보를 제공하도록 하는 신용정보법 제32조 제6항 제9호의2 및 제33조 제2항 그리고 개인정보법 제28조의2에 대하여 헌법소원을 제기하였다. 참여연대, “온 국민 건강정보조차 보험회사 등이 동의 없이 상업적으로 활용하게 한 것은 위헌- 참여연대, 신용정보법 32조6항9호의 2, 33조2항 등 헌법소원 청구 “(2020.11.3.) <<http://www.peoplepower21.org/PublicLaw/1741319>>

처리를 허용하는 신용정보법과 달리 개인정보 법상 가명정보 처리허용 목적 범위는 통계작성, 과학적 연구, 공익적 기록보존 등에 그쳐(법 제28조의2 제1항) 협소하기 때문이다. 따라서 비 신용 개인정보인 건강정보를 가명처리한 후 독자적으로 또는 금융정보 집합물과 결합하여 신용정보회사등이 [산업적] 연구목적, [상업적] 통계작성 목적으로 이용하는 것이 법에 위반되지는 않을지 의문이 제기될 수 있다.¹⁴⁾ 현행 한국 법제상 비신용 개인정보와 개인신용정보와 같이 서로다른 법의 적용대상인 정보집합물을 결합하는 경우 입법 취지상 양 법을 모두 만족시켜야 할 것이므로 신용정보법만을 거론하여 면책을 주장하기 어려울 것이다. 각종 금융산업에서 맞춤형 금융상품 설계·판촉을 위하여 비 신용 개인정보와 신용정보를 결합하려는 수요가 많을 것임에도 불구하고 이에 법적 불확실성이 존재한다.

4.3 정부의 입장: 가명처리 후 의료정보 적극 활용

4.3.1 「보건의료 데이터활용 가이드라인」의 제정

보건복지부 등은 2020년 9월 「보건의료 데이터활용 가이드라인」(이하 ‘의료데이터 가이드라인’)을 제정하여 건강정보를 가명처리하여 제3자 제공 등 ‘처리’하는 것을 허용한다는 해석을 내놓았다.¹⁵⁾ 아울러 개정위는 「개인정보 가명처리 가이드라인」(2020년 9월)도 제정하였는데 두 가이드라인 간에서 의료데이터 가이드라인이 「개인정보 가명처리 가이드라인」보다 우선 적용된다. 의료데이터 가이드라인의 주된 내용은 보건의료 데이터의 가명처리 절차, 필요한 보안조치, 가명정보 활용 및 제3자 제공시 절차 및 가버넌스, 가명정보 활용시스템 요건 등이다.

4.3.2 「보건의료 데이터활용 가이드라인」의 입장

의료데이터 가이드라인은 건강정보¹⁶⁾라도 ‘가명처리’한 후에는 정보주체의 동의 없

14) 이러한 의문은 건강정보 외 다른 비 신용 개인정보에도 동일하게 제기될 수 있다.

15) 의료데이터 가이드라인의 제정 배경으로 정부(개정위 및 보건복지부)는 의료데이터의 비식별조치를 통한 산업적 활용에 대한 법적 근거가 미비함에도 불구하고 제약이나 의료기기 등 기술, 제품 개발에 데이터 활용 필요, 의료데이터활용 및 민간개방 확대 필요, 보건의료 분야의 개인정보 활용을 위한 절차마련 필요 등을 들었다.

16) 의료데이터 가이드라인의 적용대상인 ‘건강정보’는 진료기록부 기록이나 건강검진자료는 물론, 심박수, 산소 포화도와 같이 기기를 통해 수집한 정보도 포함되며, 음성녹음과 같이 일반적으로는 건강정보로 보기 어렵지만 이를 통해 각종 질환의 위험도를 예측할 경우에는 이 역시 건강정보에 포함되는 등 매우 광범위하다.

이 목적 제약없이 활용 가능한 입장에서 제정되었다. 다만 정보주체의 동의를 요구하는 예외적 사유로, (i) 인권 및 사생활보호에 중대한 피해 야기 가능한 일부 건강정보¹⁷⁾의 활용시, (ii) 안전한 가명처리 방법이 존재하지 않는 경우라고 한다. 예컨대 음성정보 등과 같이 안전한 가명처리 방법이 개발되지 않은 경우에는 정보주체 동의를 얻어서만 활용하여야 한다.

그런데 이러한 가이드라인의 해석은 개인정보처리자가 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 하는 개인정보법 제28조의2의 해석에 있어서 의료법과의 관계에서 개인정보법 규정이 의료법의 상반 규정들보다 우선적으로 적용됨을 전제하고 있으므로 문제가 있다.

4.3.3 의료법과 개인정보법 간의 간섭

의료데이터 가이드라인은 개인정보법과의 관계를 의식하여 입장을 정리하고 있다. 우선, 타법에 대해 개인정보법의 보충성을 규정한 개인정보법 제6조에 따라, 의료기관이 보유하는 환자에 관한 기록(정보)에 대해 의료법을 우선적으로 적용한다.

의료법이 우선적용되는 경우로는, i) 의료기관이, ii) 보유 중인 iii) 환자에 관한 기록을 iv) 제3자(외부자)에게, v) 열람 또는 사본 발급 등 그 내용의 확인을 제공하는 경우이며 이 경우에는 환자 정보누설 등을 금지하는 의료법이 우선 적용된다. 따라서 이러한 경우에는 의료법에서 허용하는 사유가 아닌 이상 환자에 관한 기록 관련 정보를 제3자에게 제공할 수 없다.

그러나, 그 외의 경우 의료데이터 가이드라인은 환자 보관 진료기록과 같이 의료기관이 아닌 자(또는 기관)가 보유하는 진료기록(정보)에는 의료법이 적용되지 않는다고 하고, 나아가 가명처리하여 환자식별력이 없는 진료기록(정보)에는 의료법을 배제하고 개인정보법이 적용된다고 해석한다.¹⁸⁾ 따라서 개인정보법상 추가처리 허용규정(법제15조제3항)에 의하여 개인정보처리자는 당초 수집목적과 ‘합리적’으로 ‘관련’된 범위에서 정보주체의 동의 없이 개인정보를 추가적인 이용 또는 제공(further processing)을 할 수 있게 된다. 가명조치를 취한 개인 의료정보는 과학적 연구 등의 목적을 위한 경우 원 수집목적과의 합리적 관련성과 무관하게 개인의 동의 없이 해당 정보를 처리¹⁹⁾할

17) 이들 건강정보의 사례로는 정신질환 및 처방약 정보, 성매개감염병 정보, 후천성면역결핍증 정보, 희귀질환 정보, 학대 및 낙태 관련 정보가 있다.

18) 보건복지부, 「보건의료 데이터활용 가이드라인」, (2020.9.), 34쪽<http://www.mohw.go.kr/react/al/sal0101vw.jsp?PAR_MENU_ID=04&MENU_ID=040101&page=1&CONT_SEQ=360055>

수 있다(개인정보 법 제28조의2 제1항).

한편 신용정보법은 별개로 ‘추가처리’ 규정을 두어 양 목적 간의 관련성, 즉 원수집목적과 제공하는 목적 간의 관련성을 고려하여 당초 수집한 목적과 ‘상충’되지 아니하는 목적으로 개인신용정보를 ‘제공’하는 것을 허용하고 있다(법 제32조제6항 제9의4호). 따라서 개인 건강정보에 가명조치를 하여 신용정보집합물과 결합한 경우 개인정보법에 의하여 합리적 관련성을 요건으로 할지, 또는 신용정보법에 의거하여 ‘비(非)상충’ 요건으로 족하도록 할지 논란이 있을 수 있다.²⁰⁾ 비교법적으로 EU GDPR은 추가처리(further processing) 허용을 위하여는 원 수집목적과 해당 처리목적 간에 양립가능성(compatibility)을 요구하며(GDPR Recital 50.), 종래의 한국 법원 역시 엄격한 입장을 견지하여 왔다. 아울러 한국의 대법원도 공개된 정보라 할지라도 목적 제한 원칙상 애초에 공개된 목적에 ‘부합’ 내지 양립가능한 상황에만 활용하여야 한다는 제약을 두어 왔다.²¹⁾

이상에 비추어 현행 신용정보법은 GDPR 및 한국 법원에 비하여 정보의 활용에 치우쳐진 입장이라고 할 수 있다. 아울러 개정위와 보건복지부가 2020년 9월 제정한 의료데이터 가이드라인상 ‘과학적 연구’도 합리적으로 축소할 필요가 있다. 동 가이드라인상 과학적 연구의 범위는 (i) 자연과학적인 연구, (ii) 과학적 방법을 적용하는 역사적 연구나 공중보건 분야에서 공익을 위해 시행되는 연구 등 외에도 (iii) 새로운 기술·제품·서비스의 연구개발 및 개선 등 산업적 목적의 연구를 포함한다고 하여²²⁾ 과학적 연구의 범위를 신용정보법에 가깝게 해석론상 확장하고 있으나, 이는 ‘과학적 연구’의 문언해석을 넘는 것으로 보인다.

19) 개인정보법상 ‘처리’란 정보 이용과 제3자 제공을 포괄하는 매우 광범위한 개념으로 “개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위”로 정의된다(법 제2조 제2호).

20) 규제가 엄격한 대상과 규제가 상대적으로 느슨한 대상의 결합물을 규제할 경우 사건으로는 규제가 엄격한 대상에 적용되는 규제가 적용되어야 될 것으로 본다.

21) 대법원은 이미 공개된 개인정보일지라도 해당 정보의 수집이나 제3자 제공 등을 적법하려면 “객관적으로 보아 정보주체가 동의한 범위 내에서 처리하는 것으로 평가할 수 있는 경우”로 한정하여 해석한다(대법원 2016. 8. 17. 선고 2014다235080 판결 등).

22) 보건복지부, 앞의 가이드라인, 50쪽.

III. 적절한 정보활용 지원을 위한 법제 개선방향

1. 신용정보법의 개편: 정보보호 감독대상·주체의 일원화

현행법은 종래와 마찬가지로 개인정보법 및 신용정보법은 소관대상 및 소관 감독부서를 달리하고 있다. 그런데 개정 신용정보법에 의하면 개인신용정보의 범위가 상법상 상거래 정보로도 크게 확대되면서 개인정보와의 간섭문제가 심각하여짐에 따라 수범자의 입장에서도 적지 않은 불편이나 예측불가 상황에 놓이는 것이 가능해졌다.

이번에 신용정보법에 도입된 마이데이터업, 즉 본인신용정보관리업²³⁾과 관련하여 본인신용정보관리업자에게 제공하여야 하는 개인신용정보의 범위를 둘러싸고 적지 않은 논란이 벌어져 왔다.²⁴⁾ 본인신용정보관리업자가 개인신용정보를 보유한 신용정보제공·이용자 또는 공공기관에게 요구할 수 있는 신용정보 범위에 관하여 신용정보법 시행령이 구체적 사항을 정하고 있는데, 이번에 대통령령이 상거래 주문내역 정보를 본인신용정보관리업자에게 의무적으로 제공하여야 할 신용정보로 포함시키면서,²⁵⁾ 전자상거래업자와 금융회사들 간에 의견 충돌이 발생하였다. 개정 전의 법에 의하면 금융거래와 무관한 비금융 상거래 정보는 신용정보에 해당하지 아니하였지만²⁶⁾ 개정 신용정보법에 의하면 이를 포괄적으로 신용정보로 포섭시킴에 따라 혼선 및 종래의 기득권을 둘러싸고 이해상충이 생기게 된 것이다.

개정 신용정보법상 신용정보 범위의 대폭적 확대에 따라 양 법의 규율대상에 큰 간섭이 생겼음에도 불구하고 개인정보법은 타법에 대해 보충적으로 적용된다는 규정만을 두고 있을 뿐 합당한 해결책을 내놓고 있지 못하다. 그러나 빅데이터 시대에 해당 개인정보²⁷⁾가 비신용정보인지 신용정보인지를 일일이 구분하고 어느 법에 의한 어느 당국의

23) 본인신용정보관리업이란 일정한 신용정보를 API 등 방식을 통하여 신용정보주체가 자신의 일정한 신용정보를 조회·열람하도록 하여 개인의 신용관리를 지원하는 것을 영업으로 하는 것을 말한다(신용정보법 제2조 제9호의2 및 동법시행령 제2조제21항 및 제22항, 신용정보업감독규정 제3조의3).

24) 매일경제 (2020.10.29.), “개인이 원하면 금융사 고객 정보 마이데이터 사업자에 줘야… 예비허가만 35개사 신청, 금융사 vs 핀테크 승자는 누구?” <<https://www.mk.co.kr/news/economy/view/2020/10/1111826>>

25) 신용정보법 시행령 별표 1. 본인신용정보관리업에 관한 신용정보의 범위(제2조제22항 및 같은 조 제23항제1호 관련).

26) 2020년 2월 개정 이전의 신용정보법은 ‘신용정보’를 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 정보로 하면서도 시행령에서는 구체적인 신용정보를 금융거래 위주로 규정하고 있었으며 ‘상법상 상거래’는 신용정보의 범위로 하고 있지 아니하였다.

27) 일반적으로 건강정보는 이를 개인의 신용도를 판단하기 위한 신용정보로 보기 곤란하므로 누가 건강정보를

소관에 해당할지를 분류하는 것은 비효율적이며 사실상 불가능한 경우도 많을 것이다.

아울러 양법은 가명정보 결합시 따로 지정하는 전문기관을 통해서 수행하도록 하고 있는데, 개인정보법은 개정위 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행하도록 하고(법 제28조의3) 신용정보법은 금융위가 지정하는 데이터전문기관(법 제26조의4)을 통하도록 하여(법 제17조의2 제1항), 결합을 수행하는 전문기관이 다를 수 있다.

또한 비신용 정보집합물과 신용 정보집합물을 결합할 경우, 어느 법에 따라 원 수집목적 외 추가처리나 가명처리후 일정한 목적으로 처리가 허용되는지 법적 명확실성이 존재한다.²⁸⁾ 추가처리와 가명처리후 연구 등 목적으로 처리허용에 대해 양법 간의 허용 범위에 차이가 존재하기 때문이다. 개인정보를 관장하는 법이 양법으로 분리된 현상, 개인의 자기정보 결정권의 신장 역시 신용정보에 불가피하게 제한되는 현상으로 귀결되고 있다. 예컨대, 소위 마이데이터업이라 불리는 본인신용정보관리업, 즉 개인정보주체의 신용관리 지원을 위하여 일정한 신용정보를 수집하여 이를 개인정보주체 자신에게 제공(조회·열람)하는 영업도 신용정보법에 근거를 두고 있으므로 다룰 수 있는 정보는 ‘신용정보’에 한정될 수 밖에 없다(신용정보법 제2조 제9호의2). 아울러 본인에 관한 개인정보의 전송요구권도 개인의 자기정보 결정권을 신장시키는 장치임에도 불구하고 그 근거 조항이 신용정보법에 있기 때문에 전송요구 대상인 자신에 관한 정보가 ‘신용정보’에 그친다(신용정보법 제33조의2 제1항).

따라서 신용정보법은 신용정보회사 등에 관한 감독 사항을 중심으로 하는 감독법(업법)으로 축소 개편하여 관할부서인 금융위원회의 소관으로 두고 현행 신용정보법에 있는 개인정보 보호에 관한 사항은 개정위 소관의 개인정보법으로 이전하여 법의 규제수준 및 법 집행의 일관성 및 예측가능성을 제고할 필요가 있다. 2016년 한국이 EU 의회의 적정성 심사에서 탈락한 이유 중 하나가 개인정보보호를 위한 독립적인 감독기구 없이 방송통신위원회와 행정안전부 등으로 감독권한이 쪼개져 있었음을 지적받았던 점을 감안하면 현행처럼 두 개 부서로 관할 당국이 나뉜 상황은 EU 의회의 적정성 승인을 받는데 도움이 되지 않는다. 개인정보를 일괄적으로 개인정보법 소관으로 하여 국무총

처리하는지와 상관없이 이를 신용정보로 보아 신용정보법을 적용할 수 없을 것이며 따라서 감독주체는 여전히 개정위로 남을 것이다. 그러나 특수한 상황에서 건강정보가 개인의 신용도를 판단하는데 사용되는 것도 가능하다. 예컨대 보험금 청구·지급의 경우 질병코드 등 건강정보나 질병으로 인한 병원비·약제비 지출정보가 해당 개인의 신용도의 판단에 간접적으로 이용될 수 있는 신용정보로 볼 여지가 있을 수 있다.

28) 그러나 빅데이터의 원활한 처리를 위하여 산업계를 포함한 국민 편의, 각국이 4차 산업혁명의 주도권을 추구하는 현재 상황에 있어서 어느법 및 어느 당국의 소관인가 하는 다툼은 소모전에 불과한 것으로 여기에서 유래하는 법적 명확실성은 최소화하여 효율성을 지향해야 할 것이다.

리 산하로 소속된 보다 독립된 개정위를 감독당국으로 세우는 것이 유리할 것이다.²⁹⁾

2. 과학적·산업적 연구 목적의 합리적 제한

2.1 문제점

개인정보를 가명처리한 후 정보주체의 동의 없이 이를 이용하거나 제3자 제공을 허용하는 경우로 개인정보법은 ‘과학적 연구’ 목적을 규정한다. 개인정보법상 과학적 연구는 “기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구”로 정의된다(법 제2조 제8호). 그러나 민간투자연구 등 과학적 방법을 적용하는 연구가 의미하는 바가 무엇인지 모호하며 이를 위하여 개정위가 제정한 「가명정보 처리 가이드라인」도 애매하여³⁰⁾ 법적 불확실성이 여전히 남아 있다.

신용정보법은 개인정보법과 달리 “시장조사 등 상업적 목적”의 통계작성 목적이나 산업적 연구 목적으로도 가명처리한 개인신용정보를 처리하는 것을 허용한다(법 제32조 제6항 제9호의2). 이에 따라 가명정보 처리 가이드라인은 개인정보법상 과학적 목적의 연구마저 산업적 연구로 해석하는 입장이다. 그러나 가이드라인의 이러한 해석은 물론 산업적 연구를 허용한 신용정보법의 입법이 적정한지 논란이 가능하다.

2.2 EU GDPR

GDPR도 과학적 연구(scientific research) 목적으로 하는 추가처리를 허용하고 있지만(Art. 5(1)(b)), GDPR은 과학적 연구 목적 처리를 추가처리의 일종으로 보므로(Art.5.(1)(b)),³¹⁾ 과학적 연구 범위에 관한 논란에 불구하고 그 범위를 무작정 확대하기 곤란한

29) 한국일보, “‘데이터 3법’ 이대로는 GDPR 적정성 심사 통과 어려워”, (2019.11.13.), <<https://www.hankookilbo.com/News/Read/201911121745097280>>.

30) “‘과학적 연구에 민간정보로 분류되는 건강정보도 포함되는지, 산업적 목적 등 연구도 포함되는지가 제대로 다뤄지지 않아 모호하다”고 했다. “산업적 연구의 목적과 범위, 수행주체 등이 모호하다”며 “산업적 연구 수행 주체는 누가 될 것인지, 민간기업의 마케팅 부서가 연구를 수행해도 괜찮은 것인지 등 헷갈리는 부분이 있다”, IT조선, “데이터3법 가명정보 모호성 해결해야”, (2020.9.3.), <http://it.chosun.com/site/data/html_dir/2020/09/03/2020090303079.html>

31) GDPR은 과학적 연구 목적의 개인정보 처리를 ‘추가처리’의 유형으로 명시하고 과학적 연구 목적에 의한 처리를 원 수집목적과 양립불가능한 것으로 보지 않는다고 한다.

내재적 한계가 있었다.

그런데 최근 유럽개인정보보호감독관(European Data Protection Supervisor, 이하 ‘EDPS’)은 2020년 1월 공개한 사전의견서(Preliminary Opinion)를 통하여 과학적 연구범위를 제한하는 해석을 내놓았다. EDPS는 ‘연구’의 역할이란 다수의 사람들의 삶의 질을 향상시키고 사회적 서비스(social service)의 효율성 역시 증진시킬 수 있는 지식을 제공하는 것이라고 하여 연구의 ‘공공성’을 강조하는 해석을 하고 있다.³²⁾ EDPS의 사전의견서는 개인정보 처리에 있어서 과학적 연구목적으로 인정받아 정보 주체의 동의 없이도 정보를 처리할 수 있기 위해서 선결되어야 할 요건을 제시한다. EDPS는 과학적 연구의 수행주체가 반드시 국가나 공공기관일 것임을 요구하지 않으나, 과학적 연구 목적 처리를 위한 선결요건으로 (i) 처리대상이 개인정보이며, (ii) 관련 부문 표준 기법 및 윤리(ethics)가 적용되어야 하며, 이때 정보기반 동의(informed consent), 책임성(accountability) 및 감시(oversight)가 이에 포함된다. 그리고 (iii) 해당 연구가 사회에서 집단지식(collective knowledge) 및 복리(wellbeing)를 육성할 목적으로 수행되어야 하며, 이는 하나 또는 일부의 사적 이익(private interests)에 기여하는 것과 반대된다고 한다.

GDPR 역시 과학적 연구 목적의 개인정보 처리 범위에 대하여 기초·응용연구나 민간 펀드 연구도 포함하며 보건(public health) 부문에서 공익 목적으로 수행되는 연구도 ‘포함되어야’ 한다(Recital 159.). 과학적 연구 목적을 위한 개인정보 처리가 허용되려면, 과학적 연구 목적 맥락에서 개인정보의 공람 내지 공개가 허용되기 위하여 필요한 조건으로 특히 보건(health)의 맥락에서 과학적 연구의 결과가 ‘해당 정보주체의 이익’에 부응하는 경우를 든다(GDPR Recital 159.). 따라서 질병 팬데믹 상황에서 백신 또는 치료물질을 개발하는 연구는 주체를 불문하고 GDPR이 제시하는 과학적 연구에 해당될 수 있다.

GDPR은 해당 개인정보 주체의 이익에 부응하는 경우를 과학적 연구 목적 개인정보 처리가 허용되는 사례로 들어 과학적 연구의 공공성을 암시하고 있다. 근래 EDPS가 내놓은 해석을 함께 고려하면 GDPR이 인정하는 과학적 연구에 해당하려면 그 연구 결과는 공유되어 집단지식 수준을 높이고 다수인을 위한 보건 향상에 사용되어야 하는 공공성을 띠어야 하므로, 일부 개발 기업의 이익 추구 목적일 경우에는 과학적 연구

32) “Under the GDPR, the role of research is understood to provide knowledge that can in turn ‘improve the quality of life for a number of people and improve the efficiency of social services’. ... It is a common assumption that scientific research is beneficial to the whole of society and that scientific knowledge is a public good to be encouraged and supported.”. European Data Protection Supervisor (EDPS), “A Preliminary Opinion on data protection and scientific research”, (Jan. 6, 2020), pp.11-12.

목적을 인정받기 어려울 것이다.

2.3 미국

2.3.1 미국의 건강정보 처리

미국의 경우 개인정보 법제가 부문별로 쪼개어 있고 개인정보 보호를 일반적으로 규율하는 연방법은 없는 상황이다. 한국의 보건복지부에 상당하는 미국 HHS부 장관이 제정한 Privacy Rule³³⁾에 의하더라도 연구 수행 목적으로 정보주체의 동의없이 개인 건강정보(protected health information)를 처리하려면 상당히 까다로운 요건이 충족되어야 한다. 우선, 개인 건강정보의 이용·제공이 허용되려면, ① 해당 개인에게, ② 치료, 지불, 건강관리 서비스(health care operation)를 위하여, ③ 정보주체에 동의 또는 거절 기회를 부여하고, ④ 합리적인 보안조치를 갖춰 최소한의 정보를 이용·제공하고, ⑤ 공익 및 공공적 활동(public interest and benefit Activities) 목적으로 이용·제공되며, 그리고 ⑥ 식별자를 제거한 정보집합물 형태(limited data set)³⁴⁾로 제공되어야 한다.³⁵⁾ ‘연구’는 이 중 공익 및 공공적 활동의 일종으로 분류되어 정보주체의 동의 없이 건강정보 처리가 허용되는데 Privacy Rule은 연구에 대해서 “지식을 개발하거나 지식의 일반화에 기여하려는 체계적인 조사(any systematic investigation designed to develop or contribute to generalizable knowledge)”라고 하므로³⁶⁾ 사익 추구 목적 연구의 경우 이러한 연구에 해당한다고 적극적으로 주장하기 어려울 것이다. 또한 Privacy Rule은 정보주체의 동의 없이 연구 목적 수행을 위하여 건강정보를 원수집목적외 이용 및 제3자 제공하는 것을 허용하나, 이를 위해서는 사전에 (i) 건강정보 이용·제공 관련 해당 개인의 동의를 면제·변경하는 것에 관하여 사전에 일정한 위원회³⁷⁾의 승인을 받거나 (ii) 해당 건강정보의 이용·제공이 오직 “연구 프로토콜을 준비하거나 연구에 선행하는 유사 목적을 위한” 것임에 대한 연구자의 진술이 있어야 한다.³⁸⁾

33) 미국 법(The Health Insurance Portability and Accountability Act of 1996, 이하 ‘HIPAA’)상 HHS부의 장관(the Secretary)에게 Privacy Rule 등을 제정할 권한이 부여된다.

34) Limited data set이란, 일정한 특정 개인 및 그 친척, 가족구성원 및 피고용인들에 관한 직접적인 식별자가 제거된 보호대상 건강정보(PHI)를 말한다(Privacy Rule (6)).

35) HHS, “Summary of the HIPAA Privacy Rule”, <<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>>

36) Ibid.

37) Institutional Review Board or Privacy Board를 말한다.

2.3.2 캘리포니아 주의 개인정보 보호입법

캘리포니아 주는 개인정보 보호에 관한 일반법인 캘리포니아 소비자 프라이버시법(California Consumer Privacy Act)을 주법으로 제정·시행하고 있다.³⁹⁾ 동법은 ‘연구’를 과학적, 체계적 연구 및 관찰이라고 하면서 이를 ‘협소’하게 정의하여 동법상의 연구(기초·응용 연구 포함)란 공익을 위하여(in the public interest) 수행되는 것으로, 공중보건(public health) 분야의 공익을 위하여 수행되는 기타 다른 모든 응용 윤리 및 프라이버시법이나 연구를 준수하는 것이라고 규정한다(California Consumer Privacy Act 1798.140 본문). 캘리포니아 소비자 프라이버시법상 정보주체(소비자)의 동의 없이 개인정보를 이용하는 연구가 적법하기 위한 주된 요건으로, ① 공익 요건, 연구가 개인정보가 수집된 사업목적과 양립가능할 것, ② 이용 후 가명화 및 익명화조치를 취할 것, ③ 원 수집동의 받은 이용 목적과 양립가능한 연구에만 사용할 것, ④ 상업적 목적 용도로는 일절 사용을 ‘불허’하는 내용이 명시적으로 포함되어 있다(California Consumer Privacy Act 1798.140 각호).

결론적으로 정보주체 동의 없이 개인정보가 처리 가능한 사유로 신용정보법이 내거는 산업적 연구 목적 정보처리 허용은 개인의 자기정보결정권에 반하며 국제적 정합성 관점에서도 적정하지 아니하므로 삭제되어야 하며 개인정보법상 과학적 연구 목적의 개인정보 처리는 허용하되 그 해석은 ‘공공성’을 중시하여 해당 정보를 제공하는 정보주체의 이익과 직·간접적으로 관련되는 경우로 합리적으로 좁혀 해설할 필요가 있다.

3. 추가처리

현행 개인정보법 및 신용정보법은 정보주체의 동의 없이도 정보처리자가 개인정보의 원 수집목적 범위 외의 다른 목적으로 추가처리(further processing)를 허용하는 규정을 도입하였다(개인정보법 제15조제4항, 신용정보법 제32조제6항 제9의4호). 추가처리 규정의 도입은 GDPR의 입법례를 좇은 것인데, 추가처리를 전혀 허용하지 않을 경우 정보주체의 통상적인 합리적 의사에 부합하는 경우에도 정보이용동의를 받지 않으면 불법이 된다는 점에서 동 규정의 도입은 설득력이 있다.

그런데 추가처리 허용규정의 입법적 목적, 즉 정보주체의 합리적 의사와 부합되는

38) HHS, op cit.

39) 동법은 2018년 6월 개정되었고 2020년 1월 1일 시행되었다.

범위 내에서 추가처리가 허용되느냐이다. 개인정보법의 경우⁴⁰⁾와 달리, 신용정보법은 추가처리의 허용요건으로 “당초 수집한 목적과 상충되지 아니하는 목적”이라는 요건을 규정하여 극단적으로는 원 수집목적과 전혀 관련성이 없어도 상충되지만 않는다면 개인 신용정보를 제공하는 것을 허용하고 있다(법 제32조제6항 제9의4호).⁴¹⁾ 따라서 신용정보법의 추가처리는 추가처리 규정의 도입 목적에 맞게 적정히 축소되어야 할 것이다.

IV. 결론

2020년 8월 시행된 개정 신용정보법은 신용정보 범위를 크게 확대하여 일상생활에서의 상거래 정보를 신용정보로 포섭하였다. 그 결과 종래 잠재되어 있던 신용정보의 개인정보와의 간섭문제가 불가피하여졌다. 그러나 4차 산업혁명 시대에 개인정보의 종류가 신용정보인지 그렇지 않은지에 따라 소관법과 소관당국을 달리하는 현행법제 방식은 수범자의 혼란을 불러일으키고 법적 불확실성을 초래하게 된다. 개인정보 보호에 관한 일반법인 개인정보법이 엄연히 입법된 이상 신용정보법과 같은 특별법을 존속시켜 그만을 위한 한정된 구획에서 별도의 당국 소관의 별도 규제를 할 이유가 없다. 신용정보법을 신용정보회사 등에 관한 감독법으로 정체를 개편·확립하고 개인정보 보호에 관한 사항은 개인정보법에 통합시키고 개정위에 권한을 주어야 할 것이다.⁴²⁾ 이러한 방향을 취할 때 개인의 자기정보 결정권의 신장과 관련된 사항들을 신용정보와 비 신용정보를 일일이 구분하거나 규제차익 이슈를 논할 필요 없이 입법할 수 있을 것이다.⁴³⁾

40) 개인정보법은 “당초 수집 목적과 합리적으로 관련된 범위”를 고려하도록 하고 있으며, 개인정보법 시행령도 “1. 당초 수집 목적과 관련성이 있는지 여부” 및 “2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부”를 함께 고려할 요소로 하고 있다.

41) 다만 신용정보법시행령 제13조는 세부 사항을 규율하면서, ‘양 목적 간의 관련성, 신용정보주체로부터의 정보 수집 경위, 정보 제공이 신용정보주체에게 미치는 영향’ 등을 고려하도록 하고 있으므로 원수집목적과 전혀 관련성이 없는 목적으로는 개인신용정보를 제공하는 것은 금지함으로써 모법인 신용정보법의 문리적 해석을 상당부분 제약하고 있다.

42) 개인 ‘신용’ 정보에 관하여 특별한 규율이 필요한 일부 경우에 대하여는 개인정보법에 별도의 장이나 절을 만들어 처리하면 될 것이다. 2020년 2월 개정(8월 시행)으로 정보통신망법상 개인정보 관련 내용이 폐기·개인정보법으로 이관되면서 따로 규율할 내용은 개인정보법에 별개의 장을 신설하였는데(제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례), 개인신용정보의 경우에도 이러한 선례를 따르면 될 것이다.

43) 현행법에 새로 도입된 본인신용정보관리업(소위 마이데이터업)이나 본인에 관한 개인정보의 전송요구권도

두 번째로는 민감정보인 건강정보의 활용·제공 이슈가 있다. 의료법 등 관련법의 제동에 불구하고 건강정보를 어느 수준에서 어떠한 절차를 거쳐 허용할지 관장하는 법이 마련되어 있지 않다. 이미 살펴보았듯이 이러한 법적 불확실성은 현재 정부 입장처럼 가이드라인으로 해결될 수 있는 것이 아니므로 사회적 논의 및 입법에 의한 해결이 필요하다. 현행처럼 입법 후 드러난 사각지대를 가이드라인과 같은 정부의 ‘해석’으로 메우는 것은 유효한 대응책이 될 수 없다.

세 번째로, 과학적·산업적 연구 목적의 범위에 대해서 가이드라인⁴⁴⁾에 의할 것이 아니라 충분한 공론화를 통하여 적정한 해석론(필요시 입법)을 도출할 필요가 있다. 개인정보 수집당시 정보주체인 개인의 합리적 의사를 생각하면 자신의 개인정보가 상업적·산업적 용도로 제공·처리될 경우에는 개인의 동의를 얻도록 하는 것이 적절하다고 할 것이다.⁴⁵⁾ 또한 EU GDPR 및 근래 2020년 1월 EU데이터 보호 감독자(EDPS)가 공개한 해석, 그리고 2020년 1월 시행된 캘리포니아 소비자 프라이버시법의 동향을 참조하면, 정보주체의 동의 없이 ‘과학적 연구’ 목적으로 개인정보 처리를 허용하는 전제로 공익 내지 공공성을 요구하는 것이 타당하다.

한국법의 경우 정보주체의 동의 없이도 산업적·상업적 목적으로 개인정보 처리를 허용하는 현행 신용정보법은 조속히 개정될 필요가 있다. 아울러 ‘과학적’ 연구에 대해서는 근래 해외에서 컨센서스가 모아지고 있는 상황임을 감안하여 과학적 연구의 범위를 적절하게 해석하여야 할 것이다. 각국의 정보보호당국은 자국민의 정보가 타국으로 흘러나갔을 경우에 대응하여 해당 국가의 정보보호수준에 상당한 관심을 갖고 있다. GDPR의 예에서 보듯이 상대방 국가의 정보보호수준에 따라 자국민 정보가 흘러나가는 것을 제한하고 위반시 제재를 가하는 입법례도 있다. 개인정보 관련 입법 자체는 국내법이긴 하지만 다른 국내법과 달리 해외 주요국의 입법동향에 그 규제 수준을 맞추는 것이

등 근거 조항이 신용정보법에 있다보니(신용정보법 제2조 제9호의2 및 제33조의2 제1항), 비신용정보를 배제하고 신용정보만으로 구축해야 하는 상황이 되어 전송요구 대상이 자신에 관한 개인 ‘신용정보’ 이상으로 확대되고 있지 못하다.

44) 과학적·산업적 연구 목적의 범위에 대해서는 2016년 「개인정보 비식별조치 가이드라인」의 제정 시부터 논란이 끊이지 않아 왔다. 비식별조치 가이드라인에 담겨 있던 내용을 상당부분 반영하여 개인정보법·신용정보법이 개정된 이후에도 산업적 연구 목적 개인정보처리 허용하는 등 개인정보 처리허용 범위가 적정수준을 벗어났다는 지적을 피할 수 없다.

45) 또한 가명조치된 정보도 ‘개인정보’의 영역에 해당하므로 개인정보주체가 자신의 가명정보의 활용·제공에 대해 알고 삭제요구권 등을 가지도록 하고 목적을 다할 경우 삭제하도록 하는 등 조치를 통하여 개인정보주체와 산업적 활용의 조화를 도모하여야 한다.

유리하다.

네 번째로 추가처리에 관한 해석이다. 2020년 8월 시행된 개인정보법 및 신용정보법에 도입된 추가처리(further processing) 허용 규정은 도입 필요성이 있음에도 도입취지를 고려할 필요가 있다. 추가처리 허용규정은 결국 정보처리자와 정보주체의 편의성을 함께 고려하는 규정이지 어느 일방의 편의만을 위한 것은 아니므로 균형잡힌 입법이 필요하다. 개정 신용정보법과 같이 당초 수집한 목적과 ‘상충되지 아니하는’ 목적으로 추가처리를 허용한다면(법 제32조제6항 제9의4호), 추가처리를 허용하는 정당한 입법목적을 넘어 개인정보주체의 자기정보 결정권을 해할 가능성이 다분하다. 신용정보법상 동의 없는 추가처리의 허용 범위 역시 GDPR 및 개인정보법의 수준에 부응하는 수준으로 조율할 필요가 있다.

아울러 여러 번 강조하였듯이 현행 신용정보법에 따르면 ‘상거래’에서 발생하는 개인 정보는 신용정보로 새로이 포섭되었으므로 개인정보와 개인신용정보에 대단한 간섭이 생겼다.⁴⁶⁾ 오늘날 정보의 원활한 유통을 통한 빅데이터 활성화를 위하여 신용정보의 범위를 상거래 정보로 확장한 것이라고 주장한다면, 그와 동일한 이유로 두법은 현행과 같은 중복규제 방식으로 공존하기 어렵다.⁴⁷⁾ 달라진 시대 상황에 맞춰 개인정보 보호·활용에 관한 신용정보법상 내용은 개인정보법으로 일괄 이관하고 신용정보법은 신용정보회사 등에 관한 감독법으로 그 역할을 재정립해야 할 것이다.

46) 타 사업체가 보유한 신용정보에 대해 요구권을 갖는 본인신용정보관리업자가 요구할 수 있는 신용정보 범위에 주문정보를 포함시키는 것이 타당한지를 두고 신용정보법 시행령 개정 관련 논란이 있었다. 참여연대 공동논평, “소비자·시민단체, 금융위의 쇼핑물 ‘구매정보’ 「신용정보보호법」 ‘신용정보’로 확대해석 우려”(2020.9.8.) <<http://www.peoplepower21.org/PublicLaw/1729692>>.

47) 개인정보의 범위에 관하여 간섭·중복 여지가 매우 커진 상황에서 개인정보를 두 개의 법, 두 개의 소관 부서에 나눠 규율할 경우 수범자인 국민의 혼란이 가중되어 정보 활용에 직·간접적 비용을 초래할 것이다. 동일·유사 사항에 대하여 법과 소관부처가 나뉘어 있다보니 현재처럼 규제수준에 차등이 생기게 되고 수범자인 국민의 관점에서 또 다른 불확실성 및 불이익을 초래할 소지가 커지게 된다.

참고문헌

1. 학술지

- 양기진, “개인정보의 범위에 관한 연구- GDPR의 비식별조치와 약학정보원 사건의 검토”, 선진상사법률연구 통권 제84호, 법무부 (2018.10.), 59-92쪽.
- 전승재, “개인정보, 가명정보 및 마이데이터의 활용 범위- 데이터 3법을 중심으로”, 선진상사법률연구 통권 제91호, 법무부, 2020.7, 249-279쪽.
- 정희수, “데이터3법 개정이 금융산업에 미치는 영향”, 제후 보고서, 하나금융연구소 및 BC카드디지털연구소, 2020.7.24, 1-10쪽.

2. 인터넷자료

- 개인정보보호위원회, 「가명정보 처리 가이드라인」, (2020.9.), <<https://www.pipc.go.kr/np/default/page.do?mCode=D040010000#LIN>>, 검색일: 2020. 10. 10.
- 건치신문, “보건의료 데이터 활용 가이드라인 철회!” (2020.9.2.), <<https://www.gunchinews.com/news/articleView.html?idxno=60794>>, 검색일: 2020. 10. 8.
- 국무조정실등 5개 부서, 「개인정보 비식별조치 가이드라인」, (2016.6.) <<https://www.mois.go.kr/>>, 검색일: 2020. 9. 15.
- 매일경제 (2020.10.29.), “개인이 원하면 금융사 고객 정보 마이데이터 사업자에 줘야... 예비허가만 35개사 신청, 금융사 vs 핀테크 승자는 누구” <<https://www.mk.co.kr/news/economy/view/2020/10/1111826/>>, 검색일: 2020. 10. 9.
- 보건복지부, “보건의료 데이터 활용 가이드라인”, (2020.9.), <http://www.mohw.go.kr/react/al/sal0101vw.jsp?PAR_MENU_ID=04&MENU_ID=040101&page=1&CONT_SEQ=360055>, 검색일: 2020. 10. 9.
- 참여연대, “온국민 건강정보조차 보험회사 등이 동의 없이 상업적으로 활용하게 한 것은 위험- 참여연대, 신용정보법 32조6항9호의 2, 33조2항 등 헌법소원 청구” (2020.11.3.) <<http://www.peoplepower21.org/PublicLaw/1741319>>, 검색일: 2020. 12. 9.

- 참여연대 공동논평, “소비자·시민단체, 금융위의 쇼핑몰 ‘구매정보’ 「신용정보보호법」 ‘신용정보’로 확대해석 우려” (2020.9.8.) <<http://www.peoplepower21.org/PublicLaw/1729692>>, 검색일: 2020. 10. 15.
- 한국일보, “‘데이터 3법’ 이대로는 GDPR 적정성 심사 통과 어려워”, (2019.11.13.), <<https://www.hankookilbo.com/News/Read/201911121745097280>>, 검색일: 2020. 10. 15.
- 한국정보화진흥원, “개인정보보호 법제로 인한 빅데이터 활용 한계사례 조사·분석”, ICT 동향분석 제4호 (2015.12.), 검색일: 2020. 11. 5.
- IT조선, “데이터3법 가명정보 모호성 해결해야”, (2020.9.3.), <http://it.chosun.com/site/data/html_dir/2020/09/03/2020090303079.html>, 검색일: 2020. 9. 20.
- European Data Protection Supervisor (EDPS) (Jan. 6, 2020), “A Preliminary Opinion on data protection and scientific research”, <https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf>, 검색일: 2020. 9. 5.
- US HHS.gov., “Summary of the HIPAA Privacy Rule”, <<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>>, 검색일: 2020. 9. 10.

[Abstract]

Legal Issues Related to Proper Process of Personal Information

—Focused on Some Issues about Commercial Use of
Health Information—

GiJin Yang*

The current Korean legal system, which discriminates between the competent law and the competent authority depending on whether personal information is credit information or not, causes legal uncertainty. In particular, as Credit Information Use and Protection Act (hereinafter, CIUP Act) explicitly includes commercial information as credit information, the problem of interference with personal information of credit information, which was previously latent, has inevitably emerged. To solve this problem, as long as Personal Information Protection Act (hereinafter, PIP Act) exists as a general law on personal information protection, CIUP Act should be reorganized as a supervisory law for credit information companies, and matters related to personal information protection should be incorporated into PIP Act and authorities should be given to Personal Information Protection Commission under PIP Act.

Secondly, there is an issue of processing sensitive information such as health information. Despite prohibitions under Medical Service Act, etc., there is no law governing the legal scope and processing of health information; these legal uncertainties need to be resolved by legislation.

Thirdly, about the scope of scientific and industrial research purposes, it is necessary to legislate appropriately through sufficient public debate, not based on the guidelines. As we refer to the EU GDPR and recent interpretations published by the EU Data Protection Supervisor in January 2020, as well as California Consumer Privacy Act, in order to allow the processing of personal data for the purpose of scientific research without the data subjects'

* Professor, School of Law, JeonBuk National University

consents, it is reasonable to demand public interest or publicity.

Fourth recommendation is the appropriate legislation about further processing. In the end, the rules for allowing further processing are those that consider the convenience of the information controllers and the data subjects together, so a balanced legislation is required. However, current CIUP Act permits further processing so widely thereby highly likely undermining the data subjects' determination rights on self-information.; CIUP Act is required to be revised appropriately soon.

[Key Words] Personal information, credit information, health information, medical information, further processing, scientific research purpose