2020

사회적가치

ISSUE BRIEF

프라이버시

사회적가치

ISSUE BRIEF

프라이버시

발간사

신자유주의 경제 전략이 불러온 양극화와 불평등은 경제 패러다임의 근본적인 변화를 요구해 왔으며, COVID-19는 사회적 가치 실현을 통한 연대성과 공존의 원리를 더욱 절실하게 만들고 있습니다.

이에 한국법제연구원은 2019년 이래 지속적으로 사회적 가치 법제연구를 수행해 왔으며, 사회적 가치 창출의 극대화를 위한 다양한 논의를 견인해 왔습니다.

특히 <사회적 가치 이슈브리프> 시리즈는 우리 사회의 다양한 사회적 가치를 구체적으로 포착(捕捉)하기 위한 시도이자 심층 분야의 전문적인 집필진을 모시고 여러 차례 회의를 거듭한 결실을 담은 결과물입니다.

제2권 '프라이버시'는 헌법상 개인정보보호권에 관한 전통적인 논의를 시작으로 최근의 데이터3법 개정, 마이데이터, 정보의 수집과 윤리, COVID-19에서의 개인정보 수집과 활용 등을 관통하는 다양한 이슈에 대한 깊은 고민과 성찰을 담았습니다.

모든 집필진 여러분께 다시 한 번 깊은 감사의 말씀을 드립니다.

한국법제연구원은 향후에도 <사회적 가치 이슈브리프>를 통해 사회적 가치를 실현하는 탐색적 주제를 발굴하고, 법과 사회의 끊임없는 소통에 근간을 둔 선순환의 법제 개선 논의를 이어갈 것입니다.

여러분의 많은 관심과 성원을 부탁드립니다. 감사합니다.

2020. 10. 31.

한국법제연구원 원장 김계홍

Preface

Privacy Law in the Pandemic Year

It is an honor for me to introduce this special privacy issue of the Korea Legislation Research Institute (KLRI). It features contributions from leading South Korean privacy experts, including academics, industry experts, and legal practitioners. The essays highlight complex questions relating to privacy and data management in the 21st century. This publication appears during a privacy year like none other.

The pandemic moved our lives online and has led to ever greater collection of data. This past year has also seen the continuing development of privacy and security law along with an accompanying greater need for international cooperation. Global privacy law will be a central part of privacy law as we move forward to a post-COVID “new normal.”

Many Americans only became aware of COVID-19 once our workplaces began to shut down in March 2020. In the United States, we had the same discussions as much of the rest of the world regarding contact tracing apps, workplace safety requirements, and the security of the digital platforms on which our lives were now taking place. The results for privacy law in the United States have been mixed.

Contact tracing apps have yet to gain widespread adoption in the United States, which has limited their impact on privacy but also their potentially positive impact on stopping the spread of the coronavirus. The Federal Trade Commission reached a settlement in 2020 with Zoom, the leading platform for online meetings, based on its alleged misstatements about its security, and has required it to implement a strong information security program. As for Congress, it has failed to enact a sectoral law regulating the collection of use of personal data relating to the COVID pandemic. It also has failed to reach its longstanding goal of creating a comprehensive federal privacy law.

Despite this congressional inaction, there has been a flood of state legislation, regulations, and new case law in the United States during the pandemic year 2020-2021. California and Virginia have enacted new far-reaching privacy laws, and the California Attorney General has issued extensive regulations under the California law. There have been important judicial decisions regarding biometic privacy reached under the Illinois Biometric Information Privacy Act. And the trend of multimillion dollar settlements in consumer privacy actions continues.

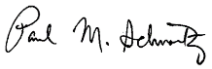
The pandemic year has also seen major privacy developments at the international level. The General Data Protection Regulation (GDPR) of the European Union continues its role as a world benchmark. Despite its Brexit, Great Britain enacted a UK GDPR and continues to regulate its personal information use according to its principles. In February 2020, Korea enacted amendments to its data protection laws and is currently engaged in "adequacy" negotiations with the European Commission. Even before these updates, Graham Greenleaf, a leading scholar of international privacy law, called the Korean data protection statute, "the most innovative data privacy law in Asia."[1] At the same time, the United States has been obliged to start new talks with the Commission due to the European Court of Justice's invalidation of its "Privacy Shield," a favored mechanism for U.S. enterprises to receive personal data from the EU.

Already in 2015, Joel Reidenberg noted the need for broad international solutions for privacy. In his view, "States must re-confront the political choice of protecting privacy as a fundamental right or protecting information as an economic commodity."[2] Reidenberg's prediction? In his

1) Graham Greenleaf, Asian Data Privacy Laws 156 (2014).

2) Joel Reidenberg, The Transparent Citizen, 47 Loyola U. Chi. L.J. 437, 462 (2015).

view, “The resolution of core, underlying privacy differences on privacy and the state’s role will need an international legal instrument to create transborder data flow stability.”[3] In the ensuing globalization of privacy law, a core requirement is for each nation, as responsible global citizen, to understand its current data processing practices as well as the necessary normative commitment to privacy as a core democratic value. This special issue on privacy helps advance this discussion in Korea, and marks an important contribution of the KLRI to the area of data privacy.



Paul M. Schwartz
Jefferson Peyser Professor of Law, Berkeley Law School
October 31, 2020

3) Id.

머리말

COVID-19 팬데믹 시대의 프라이버시

한국의 주요 국책연구기관 중 하나인 한국법제연구원의 <사회적 가치 이슈브리프 2 - 프라이버시>를 통해 여러 독자들과 인사를 나눌 수 있게 되어 영광입니다.
반갑습니다.

COVID-19 이후 프라이버시는 전세계적으로 그 어느 때보다 중요한 논쟁의 한 가운데 놓여 있습니다. 이번 이슈브리프는 정부 및 연구기관, 법학자, 법률가, 시민단체 및 민간기업을 아우르는 전문가들이 '프라이버시'에 관한 다양한 담론과 최근의 쟁점, 그리고 프라이버시에 관한 철학적 고민을 담아 집필했다는 점에서 매우 고무적입니다.

팬데믹으로 인해 우리는 삶의 많은 부분이 온라인 플랫폼으로 옮겨졌고, 결과적으로 막대한 정보 노출과 공유의 시대를 맞이하게 되었습니다. 2020년 한 해 동안 프라이버시와 보안 관련 법제 연구에는 적잖은 진척이 있기도 했지만, 개인정보 보호를 위한 국제 사회의 협력은 더욱 절실해졌습니다. 특히 프라이버시 이슈는 COVID-19 이후 뉴노멀(New Normal) 시대로 진입이 불가피해짐에 따라 전세계가 함께 고민하게 될 주제가 되었으며, (이에 따라 글로벌 차원의 법적 대응은) 향후 개인정보보호법제의 핵심 쟁점이 될 것으로 예상됩니다.

대부분의 미국인들은 지난 3월 전국적인 직장폐쇄(lock down)를 경험하고 나서야 비로소 COVID-19의 위력을 실감하기 시작했습니다. 세계 여느 나라들처럼 COVID-19 팬데믹으로 인해 미국도 확진자 동선 추적 앱(App) 도입, 직장에서의 안전지침 기준설정 및 디지털 플랫폼 보안 문제 등에 이르는 광범위한 낯선 문제들에 대해 그 어느

때보다 심각한 논의가 지속되고 있습니다. 결국 미국은 확진자 동선 추적 앱을 전면적으로 도입하지 않기로 선택하였으며, 그 결과 확진자 동선 추적 어플리케이션이 개개인의 프라이버시를 침해할 수 있는 악영향은 최소화할 수 있었습니다. 하지만 COVID-19의 신속한 확산을 저지하는 데 기여할 수 있는 순기능 또한 포기해야 했습니다.

美연방 통상위원회(Federal Trade Commission)는 화상회의 플랫폼의 선두주자인 줌(Zoom) 社를 상대로 강력한 정보 보안 프로그램 도입을 의무화함으로써 해당 플랫폼을 둘러싼 보안 문제에 대해 합의점을 찾기도 했습니다. 그럼에도 불구하고 미국 프라이버시 법제화 담론은 여전히 특별한 결론을 내리지 못한 채 공전(空轉) 하고 있는 실정입니다.

온갖 노력에도 불구하고 美의회가 COVID-19 팬데믹과 관련한 개인정보 수집을 규제하는 법안을 제정하는 데 실패함으로써 미국 연방법 차원의 포괄적인 프라이버시 보호법제 도입 성과는 미미한 수준에 그쳐 오늘에 이르고 있습니다.

이와 대조적으로 2020년부터 미국 개별 주(州) 차원의 입법안 및 규제에 관한 고민은 상당히 적극적으로 이루어져 왔으며 이 같은 움직임은 2021년, 보다 가속화될 것으로 전망됩니다. 무엇보다 새로운 판례법의 형성에 주목해야 합니다.

캘리포니아州와 버지니아州는 광범위한 프라이버시 법안을 제정했으며, 캘리포니아州 법무부장관은 주(州) 차원의 폭넓은 규제 법안을 공표했습니다. 일리노이州 법원 또한 「일리노이 생체정보보호법(Illinois Biometric Information Privacy Act, BIPA)」에 관한 중요한 판결을 내렸으며, 소비자 정보보호에 관한 수백만 달러에 상당하는 법적 분쟁들 또한 끊임없이 이어지고 있습니다.

COVID-19 팬데믹 시대를 맞아 세계 곳곳에서 굵직한 진전들 또한 주목할만합니다. 대표적으로 유럽연합의 「개인정보보호법(General Data

Protection Regulation, GDPR)」은 여전히 세계적 기준으로 기능하고 있으며, 영국은 브렉시트(Brexit)에도 불구하고 영국형 개인정보보호법을 제정하는 등 개인정보 보호를 위한 규제 체계가 전세계적으로 형성되고 있습니다.

한국의 경우 2020년 2월 「개인정보 보호법」을 비롯한 이른바 데이터 3법을 개정하고 유럽 집행위원회(European Commission)와 '적정성'에 관한 협상을 꾸준히 진행해 온 것으로 알고 있습니다. 이러한 움직임에 대하여 국제 법학자이자 프라이버시 대가인 그레이엄 그린리프(Graham Greenleaf) 교수는 "한국의 개인정보 보호법은 아시아에서 가장 혁신적인 프라이버시 보호법제"라는 평가를 내리기도 했습니다.[1)]

반면 미국은 유럽연합과 프라이버시법에 관한 협상을 새롭게 시작하지 않으면 안 되게 되었습니다. 2020년 7월 16일에 유럽사법재판소(European Court of Justice)가 유럽연합과 미국 간 도입하려고 했던 프라이버시 쉴드(EU-US Privacy Shield) 협정 체제에 대해 무효 판결을 내렸기 때문입니다. 이로써 유럽연합에 속한 국가에서 개인정보를 취득하려고 하는 미국 기업들에게 상대적으로 유리하게 작용할 수 있던 프라이버시 쉴드 체제 도입은 이제 어렵게 되었습니다.

프라이버시 법의 대가였던 조엘 라이든버그(Joel Reidenberg) 교수는 2015년에 이미 프라이버시 보호를 위해 국제 사회의 광범위한 해결책이 필요함을 시사해 왔고, 각 국가들이 프라이버시 보호를 시민의 '기본권'으로 여길

1) Graham Greenleaf, Asian Data Privacy Laws 156 (2014).

것인지, 아니면 단순히 '경제적 가치를 지닌 상품화'의 대상으로 볼 것인지에 관한 정치적인 선택을 내려야 하는 상황에 직면해야 한다고 주장했습니다.[2] 생각건대 이제라도 우리는 프라이버시 보호를 위한 국가 간의 서로 다른 접근법을 조정하고 해결하기 위해 국경 간 데이터 유통을 안정화시킬 수 있는 법적 체계 등을 논의해 나가야 할 것입니다. 프라이버시법의 세계화 시대 속에서 각 국가들은 데이터 처리(data processing)와 같은 첨단 지식에 대한 이해를 높여야 할 뿐만 아니라 민주주의에서의 중요한 가치로서의 '프라이버시'를 지키기 위한 규범적 지향을 위해 고민해야 합니다. 즉 개별 국가들이 저마다 책임감 있는 글로벌 시민이 되어 행동해야 함을 의미합니다.

그런 점에서 팬데믹 시대를 맞아 한국법제연구원이 사회적 가치로서 '프라이버시'를 선정하여 중요한 담론의 장을 열었다는 데 큰 갈채를 보냅니다. 프라이버시야말로 한국 사회뿐만 아니라 전 세계 공동체가 가장 시급하게 포착하여야 하는 묵과할 수 없는 '사회적 가치'라 하겠습니다.

2020. 10. 31.
폴 M. 슈워츠 교수(미국 U.C. 버클리 로스쿨)

Paul M. Schwartz

2) Joel Reidenberg, The Transparent Citizen, 47 Loyola U. Chi. L.J. 437, 462 (2015).

contents

SOCIAL VALUE ISSUE BRIEF

KOREA LEGISLATION RESEARCH INSTITUTE

KLRI

I

사회적 가치로서의 프라이버시

01 사회적 가치로서의 프라이버시

권건보 교수 (아주대학교 법학전문대학원)

1. 프라이버시의 의의

프라이버시(privacy)라는 말은 "사람의 눈을 피한다"라는 의미의 라틴어 'privatue'에서 유래한다.[1] 이처럼 프라이버시는 처음부터 사생활의 영역에서 파생되는 각종의 사실로서 타인에게 노출되지 않은 상태를 의미하는 것이었다. 일찍이 미국의 토머스 쿨리(Thomas Cooley) 판사가 프라이버시를 '혼자 있을 권리(right to be alone)'로 표현한 것[2]도 같은 맥락에서 이해할 수 있다.

프라이버시의 보호는 가택, 숙소 등 사적 공간의 불가침 또는 서신, 전보 등 통신의 비밀성 유지를 중심으로 법리를 발전시켜 왔다. 이는 대중의 관심으로부터 숨기거나 지킬 것이 많은 부유층이나 상류층 사람들에게 중요한 관심사가 되는 것이었다. 이러한 점에 주목하여 프라이버시의 가치가 계급적 보수성과 밀접한 관련이 있음을 지적하는 이들도 있다. 하지만 미국에서 프라이버시의 포섭 범위는 1960년대에 들어 결혼, 임신, 출산, 동성

1) 권영성, "사생활권의 의의와 역사적 변천", 「언론중재」 1983년 여름호, 1983, 14면.

2) Thomas C. Cooley, Laws of Torts, 1880, p. 29; David M. O'Brien, Privacy, Law, and Public Policy, 1979, p. 5 참조.

연애, 자녀의 양육, 교육 등의 문제에 이르기까지 개인의 사적 영역에서의 자율권 전반으로 확대되었다. 이에 따라 오늘날 프라이버시는 공간적 프라이버시(spatial privacy), 의사결정 프라이버시(decisional privacy), 정보적 프라이버시(information privacy) 등을 포괄하는 헌법상 권리로서 파악되고 있다.[3] 우리나라에서도 프라이버시는 1980년 개정 헌법에서 '사생활의 비밀과 자유'라는 이름으로 명문화된 이후, 우리 헌법상 사생활의 영역을 보호하는 일반적 기본권으로서의 지위를 인정받고 있다.

그런데 프라이버시에 포함되는 다양한 유형은 모두 개인의 사적 영역에 대한 타인의 침입이나 관심 또는 간섭으로부터 자유로운 상태를 지켜내기 위한 소극적 권리로서의 속성을 보여준다. 또한 국가가 후견적 입장에서 개인의 보호를 명분으로 개인의 삶에 간섭하거나 혹은 공공의 이익을 이유로 개인의 자율적 결정권을 억압하는 것에 대해 항의할 수 있는 권리로서 프라이버시가 원용되기도 한다(대국가적 방어권). 이 경우 프라이버시는 공권력을 상대로 개인이 자신의 자유나 권리 등 중요한 법적 이익을 지킬 수 있는 공법상의 권리로서 기능하게 된다(주관적 공권성). 프라이버시가 종종 개인적 삶의 만족도를 극대화하기 위한 사익(私益) 추구의 법적 수단으로 인식되는 것은 이러한 주관적 공권성과 무관치 않다.

하지만 프라이버시를 자신에 관한 정보의 자율적 통제, 권력에 대한 역감시, 민주적 제도에 대한 참여 등에 주목하는 견해들도 존재한다. 예를 들어 알란 웨스틴(Alan Westin)은 프라이버시를 자신에 관한 정보를 규제하고 다른 인간들과의 관계를 통제하는 시민들의 능력으로 이해하였고, 아놀드 짐멜(Arnold Simmel)은 "사회적 행동을 규율하는 가치체계의 일부"로 프라이버시를 설명한 바 있다.[4] 그리고 폴 슈워츠(Paul Schwartz)는 프라이

3) Jerry Kang, "Information Privacy in Cyberspace Transactions," 50 Stanford Law Review 1193, 1998, pp. 1202-1203.

4) Arnold Simmel, "Privacy Is Not an Isolated Freedom," in: Penneck/Chapman(ed.), Nomos XIII : Privacy, 1971, p. 71.

버시를 사회적 참여와 그에 필수적인 민주적 제도에 대한 참여로 파악하면서 여기서 개인정보 처리의 규제 필요성을 찾고 있다.[5)]

2. 개인정보 처리의 상황과 프라이버시의 위기

현대에 들어서는 사회복지국가의 이념 하에 국가기능이 점차 확대되어 왔고, 그에 따라 국가에 의한 개인정보의 수집과 활용의 필요성은 더욱 증대되었다. 더욱이 정보통신기술(ICT)이 비약적으로 고도화되면서 국민의 개인적 신상에 관한 정보를 수집하는 행정기관의 역량은 양적으로나 질적으로나 급속도로 향상되었다. 특히 대다수 국가에서 행정의 효율성과 공정성, 과학화 등을 명분으로 하여 전자정부가 구축되면서, 국가의 개인정보에 대한 관리능력이 전례 없이 강화되었다. 이에 따라 개인은 그러한 정보처리의 과정에 있어서 정보주체로서 자신의 의사를 충분히 반영할 기회를 가질 수 있어야 한다. 만일 그렇지 않으면, 개인은 자신의 내밀한 정보를 함부로 캐내서 퍼뜨리는 것을 제지할 수 없게 되고 심지어 자신에 관한 정보가 부정확하게 유포되고 있는 것을 알면서도 방치할 수밖에 없는 상황이 발생할 수 있기 때문이다. 자신의 인적 사항이나 생활상의 중요 정보가 자신의 의사와는 무관하게 집적되고 이용 또는 유통되는 상황에서는 자신에 관한 정보에 있어서조차 자율적 결정 또는 자기통제의 가능성을 봉쇄당하게 된다. 이 경우 개인의 자유로운 인격의 발현이나 사생활의 형성은 기대하기 어렵고, 그 결과 개인은 '정보의 주체'가 아니라 단순한 '정보의 객체'로 전락하고 말게 된다.

한편, 개인정보의 처리에 있어서 국가적 역량이 현격히 강화되었다는 것은 국민 개개인에 대한 감시능력이 무한히 증대되고 있음을 의미한다. 개인의 일상적 생활상이 국가에 의해 낱낱이 파악될 수 있음에도 불구하고 은밀하고 교묘하게 이루어지는 정보의 처리로 말미암아 국민 개개인으로서는 좀처럼 자신이 감시를 받고 있다거나 통제되고 있다는 것

5) Paul M. Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States," 80 Iowa Law Review 553. 1995, pp. 559-560.

을 인식할 수 없다.[6] 이러한 상태에서 개인은 어쩌면 자신이 감시당하고 있을지 모른다는 막연한 두려움을 느끼게 되고, 그 결과 개인의 자유로운 일상생활이 심각한 위축을 받게 될 수 있다. 이는 공동체 생활에 있어서 개인이 공적 의사형성의 과정에 자유로이 참여하지 못하도록 함으로써 민주적 의견형성을 저해하거나 의사를 왜곡하는 결과를 초래할 위험성까지 내포하고 있는 것이다.[7] 설령 국가나 타인에 의한 감시가 실제로 이루어지지 않는다고 하더라도, 그 감시의 가능성을 인식하는 것만으로도 개인의 일상생활이나 자율적 의사형성은 크게 위협을 받게 될 수도 있다.

나아가 빅데이터 분야에서 개인정보처리의 규모와 복잡성은 정보주체가 모든 개인정보 활용을 추적하거나 유의미한 결정을 내리는 것을 사실상 불가능하게 만든다. 또한 인공지능(AI) 기술에 의한 자동적 의사결정이 보편화된다면 개인이 정보주체로서 개입할 수 있는 여지는 현저히 줄어들게 된다. 인공지능은 개인정보가 어떻게 처리될지, 그것이 어떠한 분석결과를 가져올지에 대해 개인정보처리자도 미리 예측하기 어렵게 한다. 이로 인하여 정보주체에게 개인정보 처리의 구체적 사항을 미리 통지하는 것이 사실상 불가능하고, 따라서 정보주체는 개인정보의 활용에 대해 충분한 이해에 기초하여 동의를 제공하는 것은 기대하기 어려운 일이 되고 있다. 이러한 경우 자신에 관한 정보로부터 개인이 소외되는 현상이 가속화될 위험이 있다.

또한 사이버공간에서 잘못된 개인정보의 유통으로 개인의 사회적 정체성이 왜곡되는 경우, 그 개인이 입게 되는 피해는 예측할 수 없을 정도로 그 파장이 크다. 가령 범죄자로 오인되어 체포된다거나 신용거래 불량자 명단에 이름이 잘못 기록된다거나 한다면, 신체의 자유의 침해나 경제생활상의 피해는 말할 것도 없고 고용에 있어서의 차별, 복지수혜의 기회상실, 공동체 생활에 있어서 명예의 손상 등 그 피해는 지대한 것이다.

6) Paul M. Schwartz, op.cit., p. 553.

7) BVerfGE 65, 1 (43).

이상에서 살펴본 바와 같이 오늘날 개인정보의 처리상황은 단순한 명예훼손이나 재산적 피해와 같은 법률상 이익의 침해를 가져오는 정도에 그치지 아니하고 인격권, 재산권, 교육권, 사회보장수급권 등과 같은 기본권의 침해로까지 이어질 수 있다. 따라서 오늘날 개인에 관한 정보의 대량적 수집과 보유 및 용이한 결합은 막강한 정보권력의 남용에 따른 개인의 비인격화 내지 소외화를 초래한다는 점에서 그에 대한 통제는 개인적 차원을 넘어 매우 중대한 국가적 과제로 대두되고 있다.[8)]
이와 같은 프라이버시의 현대적 위기를 극복하기 위한 법적 대응은 오늘날 대다수의 국가에서 기본적 인권의 보장이라는 관점에서 인식되고 있다.

3. 프라이버시와 사회적 가치

(1) 오늘날 급격한 정보화의 물결 속에 프라이버시가 개인정보의 이름으로 공개시장에서 사고파는 대상이 되고 있음을 빈번하게 볼 수 있다. 이에 따라 프라이버시는 이제 인격적 가치만이 아니라 재산적 가치로서의 측면도 가지게 되었음을 부인하기 어렵다. 이는 프라이버시가 개인의 사익 추구를 위한 권리라는 인상을 강화해 주는 요인이 될 수 있다.
하지만 일찍이 찰스 프리드(Charles Fried) 교수가 간파하였듯이 개인은 자신에 관한 정보를 어떤 사람에게는 감추고 어떤 사람에게는 알려주는 방식으로 타인과의 친밀감을 조성할 수 있게 된다.[9)] 이러한 사실은 프라이버시가 개인적인 친소관계를 형성함에 있어서는 물론이고 사회적으로 폭넓은 유대관계를 설정하는 데 있어서 매우 중요한 방편이 됨을 보여주고 있다. 이러한 점에서 우리는 다시 프라이버시의 인격적 가치 또는 정서적 가치에 주목할 필요가 있다.

(2) 나아가 오늘날 프라이버시는 사회적 가치(social value)로서의 의미도 가질 수 있음에 주목할 필요가 있다. 여기서 '사회적 가치'란 매우 추상적인 개념으로 그에 대한 정의

8) 이상 권건보, 자기정보통제권에 관한 연구-공공부문에서의 개인정보보호를 중심으로-, 서울대 법학박사 학위논문, 2004, 13-15면 참조.

9) Charles Anthony Fried, "Privacy," 77 Yale L. J. 475, 1968, pp. 475, 475.

가 구구하지만,[10] "인간의 존엄성을 유지하는 기본 권리로서 인권의 보호, 사회적 약자에 대한 기회제공과 사회통합, 시민적 권리로서 민주적 의사결정과 참여의 실현 등 사회, 경제, 환경, 문화 등 모든 영역에서 공공의 이익과 공동체의 발전에 기여할 수 있는 가치"를 의미하는 것으로 정의할 수 있을 것이다.

한편 2020년 9월 10일 홍익표 의원에 의해 대표발의된 「공공기관의 사회적 가치 실현에 관한 기본법안」(의안번호: 3712) 제2조 제1호에서는 사회적 가치를 "사회·경제·환경·문화 등 모든 영역에서 공공의 이익과 공동체의 발전에 기여할 수 있는 가치"로서 인간의 존엄성을 유지하는 기본 권리로서 인권의 보호, 재난과 사고로부터 안전한 근로·생활환경의 유지, 건강한 생활이 가능한 보건복지의 제공, 노동권의 보장과 근로조건의 향상, 사회적 약자에 대한 기회제공과 사회통합 증진, 협력업체와의 상생협력 및 공정거래, 품위 있는 삶을 누릴 수 있는 양질의 일자리 창출, 지역사회 활성화와 공동체 복원, 경제활동을 통한 이익이 지역에 순환되는 지역경제 공헌, 윤리적 생산과 유통을 포함한 기업의 자발적인 사회적 책임 이행, 환경의 지속가능성 보전, 시민적 권리로서 민주적 의사결정과 참여의 실현, 그 밖에 공동체의 이익 실현과 공공성 강화 등을 포괄하는 개념으로 규정하고 있다.[11]

(3) 프라이버시가 사회적 가치와 밀접한 관련을 가진다는 점은 다음의 세 가지 측면에서 해명이 될 수 있다고 본다.

첫째, 프라이버시는 인간의 존엄성을 유지하는 기본 권리로서 인권의 보호에 기여한다. 사적인 정보가 본인의 의사에 반하여 유통되지 않도록 한다면, 개인이 자신에 관한 정보에 있어서조차 소외되어 정보의 객체로 전락하는 것을 방지할 수 있다. 특히 지능정보사회에서 인공지능(AI)이 자동적 의사결정을 통해 인간의 독자적 결정권을 대체할 경우, 개인의 인격적 정체성까지 기계에 의해 재단되는 상황에 직면하게 되어 인간으로서의 존엄

10) 김주영, "사회적 가치 법제화와 국가의 역할", 「법연」 Summer 2020 Vol. 67, 한국법제연구원, 2020. 6. 37-38면 참조.

11) http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_V2J0P0A9O1Q0J1M1F4Q8S2H-0J7P6L9 (2020. 10. 24. 방문) 참조.

성과 가치는 유명무실한 것이 되고 말 것이다. 그런데 최근 시행된 유럽연합의 개인정보 보호법(General Data Protection Regulation, GDPR)은 자동적 의사결정의 대상이 되는 것에 반대할 수 있는 권리가 정보적 프라이버시의 새로운 내용으로 포함될 수 있음을 보여주고 있다. 이에 따르면 프라이버시는 전통적인 공권력은 물론이고 장래의 새로운 기술권력 또는 정보권력에 대항하여 인간의 존엄권을 보호하는 수단이 될 수 있을 것이다. 이러한 점에서 프라이버시는 새로운 인권 침해의 위협에 대항하는 장치로서 사회적 가치를 실현하는 데 중요한 역할을 할 수 있다.

둘째, 프라이버시는 사회적 약자에 대한 기회제공과 사회통합에 이바지한다. 사회국가원리 혹은 사회복지국가 시스템 하에서 개인정보는 국가의 생존배려를 받기 위한 대가로 지불해야 할 비용처럼 인식되는 경향이 있다. 사회보장을 받기 위해 어쩔 수 없이 개인정보를 제공해야 하는 사회적 약자들의 입장에서는, 프라이버시에 대한 보호를 충분히 신뢰할 수 있을 때 비로소 사회보장을 받을 권리가 실질적으로 보장된다고 느낄 수 있을 것이다. 따라서 오늘날 프라이버시 보호는 사회적 약자의 보호를 위해서도 중요한 의미를 가질 수 있다. 이러한 측면에서도 프라이버시는 사회적·경제적·문화적 영역에서 공공의 이익과 공동체의 발전에 기여할 수 있는 가치로서 인식될 수 있다.

셋째, 프라이버시는 시민적 권리로서 민주적 의사결정과 참여의 실현에도 기여한다. 개인에 대한 감시는 개인의 존엄성과 자율성을 위축시킬 뿐만 아니라, 공동체생활에 있어서 개인이 공적 의사형성과정에 자유로이 참여하지 못하도록 한다. 이는 결국 민주적 의견형성을 저해하거나 의사를 왜곡하는 결과를 초래할 수도 있다. 정보적 프라이버시는 자신에 관한 정보의 열람, 정정, 처리정지 등을 요구할 수 있는 권리를 내포하므로, 개인은 이를 통해 국가의 시민사회에 대한 감시체계의 운영 상황을 파악하고 그에 대해 견제할 수 있다. 따라서 개인의 정보적 통제권은 국가의 정보활동을 역으로 감시하는 역할을 할 수 있으며, 이를 통해 비판적 시민의식을 함양하고 민주적 의사결정에 적극적으로 참여할 수 있는 기회를 부여할 수 있다. 이러한 측면에서 프라이버시는 민주적 의사결정과 참여를 증진하는 역할도 하게 되므로 사회적 가치로서의 의미를 가지게 된다.

4. 결어

그동안 프라이버시는 공공의 이익을 실현하기 위한 공권력의 투입에 대항하기 위한 사익의 옹호 수단으로서 인식되는 경향이 있었다. 이러한 관점에서 프라이버시는 얼핏 사회적 가치와 대척점에 있는 것으로 보일 수도 있다. 하지만 시민이 자유를 억압하는 권위주의적 통치로부터 개인의 존엄성을 확보하고 억압과 배제, 차별로부터 시민과 소수자를 지켜내는 민주적 기제로 프라이버시가 작동해온 것도 부인하기 어렵다. 더욱이 지능정보사회에서 프라이버시는 인권의 보호, 사회적 약자에 대한 기회제공과 사회통합, 민주적 의사결정과 참여의 실현 등을 위한 보다 적극적인 역할을 요구받게 될 가능성이 높다. 이렇게 볼 때 프라이버시는 그동안 다양한 공적 이익의 실현에 상당한 기여를 해왔으며 앞으로도 새로운 차원에서 사회적 가치의 실현에 이바지할 수 있다는 점에서 우리 사회에서 매우 중요한 의미를 갖는 기본권이라고 할 수 있다.

프라이버시 관련 법제의 발전을 위해서는 전통적인 공권력은 물론 새로운 정보통신기술의 지배적 권력에 맞서 모든 개인이 공동체의 동등한 구성원으로서 민주적 의사결정에 적극적으로 참여하고 대량적 정보처리와 자동적 의사결정에 있어서 인간의 대상화를 방지할 수 있는 방안을 꾸준히 모색해나가는 것이 중요하다고 본다. 바로 여기서 프라이버시의 미래, 즉 우리 사회에서 지속적으로 프라이버시가 사회적 가치로서 공공의 이익과 공동체의 발전에 기여할 수 있는 길을 찾을 수 있을 것이다.

KOREA LEGISLATION RESEARCH INSTITUTE

KLRI

II

민주사회 원리로서의 프라이버시의 역할

01 실명사회와 프라이버시권

오병일 대표 (진보네트워크센터)

1. 서론

코로나19에 대한 한국의 방역 정책이 성공적인 것으로 전 세계적인 평가를 받고 있다. 한국 정부가 'K-방역모델'을 '①검사·확진→②역학·추적→③격리·치료'로 이어지는 3T(Test-Trace-Treat)로 표현한 것과 같이, 이는 감염병 환자에 대한 역학조사를 통해 접촉자를 파악하고 적극적으로 진단 검사를 시행하는 것에 기반하고 있다.[1] 한국은 역학조사 과정에서 신용카드 및 교통카드 이용내역, 휴대전화 위치정보, CCTV 정보 등을 수집하고 있을 뿐만 아니라 기지국 수사 방식을 이용한 저인망식 접촉자 추적, 앱 및 전자팔찌를 통한 자가격리자 감시, 전자출입명부 시스템 등을 통한 시설 출입기록 작성 의무화 등의 정책을 시행하고 있다. 다른 나라에서도 감염병 대응 과정에서의 개인정보 이슈가 불거지고 있기는 하지만, 한국처럼 방대한 개인정보 수집과 다양한 감시 기술을 사용하고 있는 나라는 거의 없다. 그 배경에는 메르스 사태를 거치면서 「감염병의 예방 및 관리에 관한 법률」에 이미 그에 관한 법적 근거를 마련할 수 있었다는 점, 프라이버시에 대한 국민들의 인식이 상대적으로 덜 예민한 편이라는 점 등 여러 요인이 있겠으나, 그러한 방역

1) 산업통상자원부 보도자료, "'K-방역모델'을 세계의 표준으로 만들 길잡이 나왔다 : K-방역 3T (Test-Trace-Treat) 국제표준화 추진전략(로드맵) 발표", 2020. 6. 11.

모델을 가능하게 했던 물질적인 조건이 갖추어진 사회적인 여건을 빼놓을 수 없을 것이다. 즉, 신용카드 및 교통카드 사용의 보편화, 광범한 CCTV 설치, 휴대전화 실명제 등 특정 개인을 식별하고 과거 행적을 추적할 수 있는 시스템이 존재하고 있다는 것이다.

물론 새로운 기술과 서비스의 발전에 따라 과거보다 프라이버시 및 개인정보 침해 위협이 더욱 커진 것은 비단 한국만의 현상은 아니다. 예를 들어 생체인식이나 사물인터넷을 통한 개인정보 수집과 같이 과거에는 없었던 새로운 데이터의 생성, SNS를 통한 자발적인 개인정보의 공유, 신용카드나 인터넷 접속기록과 같이 삶의 궤적 자체가 기록되는 것으로 인한 빅데이터 생성, 정보주체가 인지하지 못하는 사이에 이루어지는 개인정보 수집, 글로벌 인터넷 서비스의 보편화에 따른 개인정보의 국제 이전 활성화 등의 경향은 전 세계적인 현상이다. 그러나 현존하는 특정 개인에 대한 식별체계에 의존하여 개인정보 처리가 이루어지는 환경은 전 세계적으로 공통된 것이라고 보기 힘든, 한국에서의 고유한 측면이며 이는 한국에서의 개인정보 침해 위협이 훨씬 커지는 요인으로 작용하고 있다. 보편적 개인식별자를 통해 서로 다른 개인정보가 연계되어 특정 개인의 식별가능성이 커질 뿐만 아니라, 개인정보 유출이나 남용으로 인한 피해가 특정 개인에게 직결되기 때문이다. 물론 사건 현장의 DNA나 인터넷 로그 기록 등 파편화된 개인정보 조각들을 통해 특정 개인에 대한 추적이 불가능한 것은 아니지만, 아예 사전적으로 모든 사람의 DNA 데이터베이스를 구축해 놓거나 통신 이용자의 신원정보를 보유하는 것을 동일하게 볼 수는 없다.

이런 측면에서 한국은 실존하는 개인에 대한 고유 식별자와 본인인증 시스템을 통해 언제라도 특정 개인을 추적 가능한 방식으로 개인정보의 수집 및 처리가 이루어지는 환경을 구축하고 있다. 본인의 실제 이름이 사용되는 것은 아니지만, 실존하는 개인의 본인확인에 기반하고 있다는 점에서 가히 한국을 '실명사회(實名社會)'라고 할 수 있을 것이다. 그리고 실명사회를 구현하기 위한 주된 제도적인 수단이 주민등록번호, 휴대전화 실명제, 본인확인기관 제도와 연계정보(CI)이다.

2. 주민등록번호 제도

한국에서 실명사회의 가장 기반이 되는 제도는 주민등록번호 제도이다. 이를 통해 한국의 모든 개인이 식별되고 개인정보가 관리·연계되며 궁극적으로 추적될 수 있기 때문이다.

주민등록번호의 근거법률인 「주민등록법」은 1962년에 제정되었지만, 주민등록번호는 1968년 「주민등록법 시행령」에서 처음 규정되었다. 주민등록증의 일제 발급과 동시에 발급대상자에게 고유한 12자리 번호를 부여하면서 도입된 것이다. 이후 1975년 「주민등록법」 제3차 개정으로 오늘과 같은 13자리 주민등록번호 체계로 변경되었다. 「주민등록법」에 주민등록번호가 명문화된 것은 1980년 제5차 개정을 통해서이며, 주민등록번호 부여의 법적 근거를 명확하게 규정한 것은 2001년에 이르러서였다. 현행 「주민등록법」은 제7조의2 제1항에서 "시장·군수 또는 구청장은 주민에게 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다."라고 규정하고 있지만, 구체적인 부여 방법은 대통령령에 위임하고 있다. 그런데 「주민등록법 시행령」 제7조에서도 구체적인 부여 방법을 정하고 있지 않으며, 「주민등록법 시행규칙」 제2조에서야 "생년월일·성별·지역 등을 표시할 수 있는 13자리의 숫자로 부여한다."라고 규정하고 있지만 그 조합 방법에 대해서는 언급이 없다.[2)]

주민등록번호는 모든 국민에게 출생시에 의무적으로 부여되고 사망할 때까지 (극히 예외적인 경우를 제외하고는) 변경할 수 없는 국민식별번호이다. 근거 법률의 목적[3)]에 맞게 수집, 활용되어야 하지만, 주민등록번호는 행정, 복지, 조세, 교육, 의료, 금융, 통신 등 공

2) 김민호, "정보사회에서 주민등록제도와 개인식별번호체계의 공법적 쟁점", 「공법연구」 제40집 제1호, 2011, 360-361면.

3) 「주민등록법」 제1조는 법의 목적을 "주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것"으로 규정하고 있다.

공 및 민간 부문에서 상당히 광범하게 수집·활용되어 왔다. 국가인권위원회는 주민등록번호의 기능과 특성을 다음과 같이 정리하고 있다. 첫째, 각 개인마다 고유하고 변하지 않으며 강제적으로 부여됨에 따른 '표준적인 식별기능', 둘째 특정 문서나 기관에서 본인여부를 인용하여 증명하게 한다는 점에서 '인증수단'의 역할, 셋째 모든 정보에 접근하기 위한 '만능열쇠' 또는 '연결자' 기능, 넷째 생년월일, 성별, 출신지역 등의 내용을 담고 있어 개인의 특성을 묘사하는 기능.[4)]

애초에 주민등록번호를 포함한 주민등록제도 자체가 군사독재 시절에 주민통제의 목적으로 도입된 것이기는 하지만, 1990년대 이후 정보화의 진전에 따라 주민등록번호로 인한 문제가 더욱 심화되었다. 이에 대해 국가인권위원회는 "정부와 공공기관 등이 보유하고 있는 방대한 개인정보가 서로 연결되어 있어 주민등록번호만 입력하면 대상자의 개인정보를 쉽게 취합하고 확인할 수 있으므로 수시로 타기관의 정보요청대상이 될 뿐만 아니라 불법적인 방법을 통한 정보유출이나 내부직원의 무단 열람이 발생하는 등 남용되거나 악용될 가능성을 배제할 수 없"으며, 민간영역에서도 개인정보 유출이 "보이스피싱과 같은 사기형 범죄, 개인피해 범주를 넘어 신용시스템 자체를 위협하는 범죄 등에 악용되고 있어 향후에도 다양한 형태의 범죄에 이용될 개연성"이 있다고 지적하였다. 또한, "대다수 인터넷 업체들이 주민등록번호를 포함한 개인정보에 기반하여 실명제를 채택하고 있기 때문에, IP주소와 행위자의 신원이 결합되어 온라인 행위추적이 곧 특정인의 개인정보에 대한 추적이 될 수 있음"을 우려하고 있다.[5)] 주민등록번호의 위헌성도 학계에서 끊임없이 지적되어 왔는데, 주민등록법에서 주민등록번호 운영을 위해 필요한 법률적 규율사항을 갖추지 못하고 있다는 법률유보의 원칙 위배의 문제뿐만 아니라, 명확성 원칙 및 포괄위임금지의 원칙에도 부합하지 못하다는 비판이 제기된다.[6)]

4) 국가인권위원회, "주민등록번호제도 개선권고", 2014. 8. 5. 결정, 4-5면.

5) 앞의 국가인권위원회 결정, 6-8면.

6) 이장희, "주민등록번호제에 대한 헌법적 쟁점", 헌법재판소 헌법재판연구원, 2013. 2., 100면.

그 특성과 문제점을 고려했을 때, 주민등록번호 제도의 근본적인 개선 방안은 다음 세 가지로 정리할 수 있다. 첫째, 주민등록번호의 사용 제한, 즉 주민등록관련 행정업무와 사법행정업무에 한정하여 사용하고 다른 공공영역에 대하여는 목적별 자기식별번호 체계를 도입할 것, 그리고 민간영역에서도 주민등록번호의 사용을 최소화할 것. 둘째, 개인정보를 포함하지 않는 임의번호로의 번호체계 변경. 셋째, 주민등록번호의 변경절차 마련.[7)]

국가인권위원회가 위와 같은 권고를 한 것은 2014년이지만 아직까지 주민등록번호 제도의 근본적인 개혁은 이루어지지 않고 있다. 다만, 대량 개인정보 유출사고가 발생하고 주민등록번호 제도의 문제점이 지적되면서 조금씩 개선이 이루어지고 있다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정으로 2013년 2월 17일부터 정보통신망에서의 주민등록번호 수집이 금지되었고, 2014년 8월 7일부터는 사회 전 영역에서 법령에 근거가 없이는 주민등록번호를 수집할 수 없도록 하는 '주민등록번호 수집 법정주의'가 도입되었다.[8)] 2015년 12월 23일에는 헌법재판소가 주민등록번호 변경에 관한 규정을 두고 있지 않은 「주민등록법」 제7조에 대해 헌법불합치 결정을 내렸다. 주민등록번호의 유출로 인해 발생할 수 있는 피해 등에 대한 아무런 고려 없이 주민등록번호 변경을 일률적으로 허용하지 않는 것은 그 자체로 개인정보자기결정권을 침해한다는 것이다.[9)] 이후 2016년 5월 19일, 「주민등록법」 개정안이 국회를 통과하였는데 국가인권위원회의 권고에 따라 주민등록번호 제도의 근본적인 개선을 요구했던 시민사회의 바람과 달리, 헌법재판소 결정의 대상이 된 주민등록번호의 변경만을 다루었다. 그나마 주민등록번호의 변경이 가능한 경우 역시 유출로 인해 생명·신체 및 재산, 성폭력 등과 같은 피해를 입거나 입을 우려가 있는 경우로 한정하였다.[10)] 2017년 5월 30일, 주민등록번호 변경 여부 심사를 위해 행정안전부 소속으로 주민등록번호변경위원회가 출범하였다.

7) 앞의 국가인권위원회 결정, 1면.

8) 안전행정부 보도자료, "주민등록번호, 이제는 함부로 수집하지 못한다! - 안행부, 8월 법시행 대비 가이드라인 배포, 민·관 합동캠페인 전개 -", 2014. 1. 20.

9) 헌재 2015. 12. 23. 2013헌바68 등, 주민등록법 제7조 제3항 등 위헌소원 등 [헌법불합치].

10) 경실련 시민권익센터 등, "미완으로 끝난 주민번호 개선, 20대 국회서 바꿔야!", 「19대 통과된 주민등록법에 대한 시민사회단체 입장」, 2016. 5. 19. http://act.jinbo.net/wp/9538/ (최종방문일 2020. 8. 10.)

3. 휴대전화 실명제

휴대전화 실명제는 휴대전화 서비스를 사용하고자 하는 이용자에 대해 본인확인을 의무화하는 제도를 의미한다. 통신사는 본인확인기관으로도 지정되어 있기 때문에 본인확인 과정에서 수집한 주민등록번호도 보유하고 있다. 휴대전화 실명제를 통해 특정 개인의 주민등록번호, 휴대전화 번호, 단말기 인증번호(IMEI), 가입자 식별번호(USIM), 온라인 이용기록 등이 언제든지 추적될 수 있도록 연계된다. 기존의 전화나 컴퓨터와 달리 대부분의 모바일 기기는 특정 개인이 전용으로 사용하기 때문에, 휴대전화 번호나 단말기 정보로 기록된 온라인 활동의 흔적들은 특정 개인의 활동 기록으로 쉽게 추정될 수 있다. 갈수록 모바일 기기를 통한 인터넷 활용의 비중이 증가하고 있는 경향을 고려할 때 휴대전화 실명제가 개인의 프라이버시에 미치는 영향은 엄청나다고 할 수 있다.

휴대전화 실명제의 법적 근거는 「전기통신사업법」 제32조의4(이동통신단말장치 부정이용 방지 등) 제2항이다. 이에 따르면 이동통신사업자는 서비스 제공 계약 체결시 부정가입방지시스템 등을 이용하여 본인 여부를 확인해야 하고, 본인이 아니거나 본인 여부 확인을 거부하는 경우 계약의 체결을 거부할 수 있다. 그리고 동법 제32조의5(부정가입방지시스템 구축)에 의하면 과학기술정보통신부 장관은 부정가입방지시스템을 구축하여야 하고 이동통신사업자들이 본인확인을 위해 이 시스템을 이용할 수 있도록 하여야 하는데, 이 시스템의 구축 및 운영을 위해 행정정보 공동이용 시스템을 활용할 수 있도록 하여야 한다.

위의 조항들은 2014년 10월 15일 「전기통신사업법」 개정으로 신설되었지만, 사실 그 이전에도 통신사들은 가입자의 본인확인을 해오고 있었다. 「전기통신사업법」 제50조(금지행위) 제5항 및 동법 시행령 제42조 제1항은 이용자의 가입의사를 확인하지 않고 전기통신역무의 이용계약을 체결하는 행위를 금지하고 있었기 때문이다.[11] 위 개정을 통해 본

11) 과학기술정보통신부, “헌법소원(2017헌마1209) 관련 부처의견 검토”(2018. 1. 5.), 2면 참조.

인확인 의무를 강화한 것은 아이러니하게도 2014년 초에 있었던 카드3사의 대량 개인정보 유출 사고 이후에 이용자의 개인정보를 보호하기 위한 명분으로 한 것이었다. 현금을 지급하거나 대출을 해주는 조건으로 휴대전화를 개통하여 넘겨받는 '휴대전화 개통사기' 또는 사망자, 완전 출국 외국인의 명의 또는 위조신분증을 통해 휴대전화를 부정개통하여 범죄에 악용하거나 해외로 밀반출하는 행위 등 '타인명의의 휴대전화 개통'을 방지하겠다는 것이다.

그런데 이처럼 악의적인 목적으로 타인명의의 휴대전화를 개통하려는 행위가 발생하는 이유는 사실 '휴대전화 실명제'에 기반하여 서비스가 제공되기 때문이다. 애초에 휴대전화 서비스를 사용하기 위해 가입자 명의가 중요하지 않고 본인확인을 하지 않는다면, 굳이 타인의 명의를 도용하여 휴대전화를 개통할 이유가 없어진다. 즉, 문제를 야기하는 조건(휴대전화 실명제)을 해소하는 방식이 아니라 오히려 그 조건을 강화하는 방식으로 문제를 풀었던 것이다. 물론 그 이유는 범죄수사의 편의를 위해 휴대전화 실명제를 포기할 수 없었기 때문일 것이다. 반면 이용자, 시민의 입장에서는 언제든지 내 휴대전화를 통한 모든 활동 기록들이 추적될 수 있는 상황에 놓인 것이다.

통신 서비스를 제공하기 위해 본인확인은 필요하지 않다. 우리가 해외에 나가서 유심칩만 구매하면 통신 서비스를 이용할 수 있는 것도 이 때문이다. 후불제의 경우에도 요금납부를 보장할 수 있다면 반드시 본인확인이 필요한 것은 아니다. 따라서 휴대전화 실명제는 서비스 제공 목적이 아니라 다른 공공적 목적, 즉 범죄수사의 편의를 위해 도입된 정책으로 볼 수 있다. 그러나 특정한 범죄수사를 위해서가 아니라 모든 사람을 잠재적인 범죄자로 간주하고 언제든지 추적할 수 있는 환경을 구축한다는 점에서 그동안의 인권 원칙에 부합하는지 의문이다.[12] 시민사회는 휴대전화 실명제가 익명통신의 자유, 이용자의 프라이버시 및 개인정보자기결정권을 침해한다고 비판하고 있다.[13]

12) 마찬가지로 서버의 로그 기록의 보관을 의무화하는 소위 통신사실확인자료 보관 의무화(Data Retention) 제도 역시 전 세계적으로 논란이 되고 있다.

13) 프라이버시 특보 방한을 위한 시민사회단체 네트워크, 유엔 프라이버시 특보 방한을 위한 한국 시민사회 보고서, 2019.7. 36면.

2017년 11월 1일, 사단법인 오픈넷은 휴대전화 실명제에 대해 헌법소원을 제기하였으나, 2019년 9월 26일 헌법재판소는 7:2로 합헌결정을 내렸다.[14] 휴대전화 실명제가 익명통신의 자유와 개인정보자기결정권을 제한함을 인정하면서도 과잉금지 원칙에 반하지 않는다고 본 것이다. 그러나 재판관 이석태와 김기영은 위헌 취지의 반대 의견을 통해, "차명휴대전화 또는 익명휴대전화를 이용하고자 하는 자가 언제나 범죄의 목적을 가지는 것도 아니며, 자신의 신원을 밝히지 아니하고 이동통신서비스를 이용하고자 하는 사람들에게는 기자의 취재원 보호, 변호사의 의뢰인 비밀 유지, 내부고발자, 인권활동가, 목격자 등의 보호, 개인정보 유출 우려, 불법 도청·감청으로 인한 피해 방지 등의 다양한 사유가 존재할 수 있다. 요컨대 익명통신은 도덕적으로 중립적인 것이므로, 차명휴대전화 또는 익명휴대전화를 금지하는 것 자체는 개인정보자기결정권 및 통신의 자유를 제한하기 위한 정당한 입법목적이 될 수 없다"라고 설시하였다.[15] 또한, "익명성은 타인에게 노출될 위험 없이 통신을 할 수 있는 사생활의 자유 영역을 형성하는 기능을 갖는다. 현대사회에서 익명통신은 이용자가 자신의 통신의 비밀과 자유를 보호하기 위하여 취할 수 있는 소수의 수단들 중 하나로서 중요한 의미를 갖는 것이다."라고 하면서,[16] 그럼에도 휴대전화 실명제는 익명으로 이동통신 서비스를 이용할 가능성을 완전히 배제하여 그 제한이 중대하다고 보았다.[17]

14) 헌재 2019. 9. 26. 2017헌마1209, 전기통신사업법 제32조의4 제2항 등 위헌확인 [기각].

15) 헌재 2019. 9. 26. 2017헌마1209, 판례집 31-2상, 340면, 364-365면.

16) 위 판례집, 369면.

17) 오픈넷, "전기통신사업법상 휴대폰 실명제 합헌 결정 유감", 2019.11.8. https://opennet.or.kr/16787 (최종방문일 2020. 8. 10.)

4. 본인확인기관제도와 연계정보

연계정보(Connecting Information, CI)는 주민등록번호를 일방향 암호화하여 생성되는 고유식별번호로서, 이용자 본인확인 시 본인확인기관이 생성하여 온라인 사업자에게 제공한다.[18] 2013년 2월 17일부터 정보통신망에서의 주민등록번호 수집이 금지되었지만, 사업자들은 주민등록번호와 1:1 매칭되는 연계정보(CI)를 통해 실존하는 개인을 식별할 수 있다. 서로 다른 사업자들이 연계정보(CI)를 통해 동일한 이용자를 식별할 수 있기 때문에 연계정보(CI)는 주민등록번호와 같은 연계키로 기능한다. 온라인에서의 이용자의 행적은 연계정보(CI)와 주민등록번호를 통해 언제든지 추적 가능해진다.

인터넷 실명제(본인확인제)는 한국의 대표적인 갈라파고스 규제 중의 하나이다. 2006년 12월 22일, 인터넷 실명제(제한적 본인확인제) 도입을 내용으로 하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 개정안이 국회를 통과하기 이전부터 상당수 인터넷 사업자들은 관행적으로 본인확인을 하고 있었다. 2000년대 초반에는 이름과 주민등록번호를 대조하는 방식의 본인확인 방법이 널리 활용되었으나 주민등록번호 유출로 인한 문제가 이슈가 되자, 정부는 사업자들로 하여금 주민등록번호를 수집하지 않는 다른 본인확인방법(주민번호 대체수단)을 제공하도록 유도하였고, 이는 2008년 6월 13일 정보통신망법 개정을 통해 의무화되었다. 아이핀(i-PIN) 서비스는 주민번호 대체수단으로 2005년 10월에 처음 도입되었다. 그런데 기존 아이핀의 경우 이용자 식별번호로서 '중복가입확인정보(Duplication Information, DI)'를 생성하였는데, 문제는 웹사이트 별로 DI 값이 상이했기 때문에 서로 다른 서비스 사업자들 사이에 동일한 이용자를 대상으로 한 연계 서비스를 할 수 없었다. 이러한 문제를 해결하기 위하여 정부는 2009년 7월 아이핀 2.0을 도입했는데 아이핀 2.0은 공통 식별자인 연계정보(CI)를 생

18) 한국인터넷진흥원, "CI에 대한 현황 및 논의 필요사항", 2019. 7. 26.「CI(연계정보)에 대한 의견수렴회」발제문, 6면.

성하였다.[19] 서비스 제공자들은 본인확인기관으로부터 i-PIN 번호 외에도 이용자의 성명, 생년월일, 중복가입확인정보(DI), 연계정보(CI), 성별, 연령대, 내·외국인 정보 등을 제공받는다.

2012년 8월 23일 정보통신망법상 본인확인제에 대해 헌법재판소가 위헌 결정을 내렸다.[20] 「공직선거법」상 인터넷 실명제(제82조의6)의 경우, 2010년에는 합헌 결정이 나왔지만 2021년에는 결국 위헌 결정이 내려졌다(헌법재판소 2021. 1. 28. 결정, 2018헌마456, 2018헌가16, 2020헌마406). 그러나 「청소년 보호법」상 청소년유해매체물 판매 등 관련 나이 및 본인확인(제16조 제1항), 「게임산업진흥에 관한 법률」상 게임 이용자의 회원가입 시 본인확인(제12조의3 제1항 제1호) 등 여전히 본인확인을 의무화하는 법률이 존재한다. 또한 정보통신망법상 본인확인제가 위헌이라고 하더라도, 사업자가 본인확인 시스템을 자발적으로 채택하는 것까지 금지되는 것은 아니다. 정보통신망법 제23조의3은 여전히 방송통신위원회가 본인확인기관을 지정할 수 있도록 하고 있으며, 현재 신용정보업체, 통신사, 신용카드사 등이 본인확인기관으로 지정되어 있다. 또한 2013년 2월 17일부터 정보통신망에서의 주민등록번호 수집이 금지되었음에도 불구하고, 본인확인기관은 주민등록번호를 수집할 수 있다(정보통신망법 제23조의2 제1항 제1호).

본인확인을 요구하는 법제, 본인확인기관의 지정, 연계정보(CI)의 활용 등이 서로 맞물려 있는 듯이 보이지만, 현재와 같은 시스템의 구축이 필연적인 것은 아니다. 우선, 청소년보호법 등 본인확인을 요구하는 법제의 타당성은 별개로 논의할 필요가 있겠지만, 그러한 법률이 존재한다고 현재와 같은 본인확인기관 제도가 있어야 하는 것은 아니다. 즉, 본인확인을 어떻게 할 것인지는 각 서비스 사업자들이 자신의 서비스에 가장 적합한 방식

19) 방송통신위원회, 주민번호 외 회원가입수단 도입 관련 정책설명회(2010.2.1.) 발표 자료, 22-27면. 출처: https://www.kisa.or.kr/uploadfile/201002/201002021155389366.pdf (최종방문일 2020. 8. 10.)

20) 헌재 2012. 8. 23. 2010헌마47 등, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 제1항 제2호 등 위헌확인 [위헌].

을 선택하도록 할 수 있고 또한 본인확인 서비스를 제공하는 업체도 자율적으로 경쟁할 수 있도록 놔둘 수 있을 것이다. 그럼에도 우리나라는 방송통신위원회가 본인확인기관을 '지정'하고 민간기업임에도 불구하고 이들에게는 주민등록번호를 수집할 수 있는 특혜를 주었다. 이는 한국이 주민등록번호에 기반한 본인확인만을 고집하는 것에 기인한다.

둘째 본인확인을 요구하는 법제가 있다고 하더라도, 연계정보(CI)의 생성이 반드시 필요한 것은 아니다. 본인확인기관은 서비스 사업자의 이용자가 본인이 맞는지, 혹은 특정 연령 이상인지 여부만 알려주면 충분하다. 애초에 연계정보(CI)는 물론이고 중복가입확인정보(DI) 역시 본인확인기관이 서비스 사업자에게 알려줄 것을 법에서 요구하는 것은 아니다. 연계정보(CI)가 도입된 이유는 서로 다른 업체간에 동일 이용자를 식별할 수 있도록 하여 제휴 서비스 제공을 용이하게 하고자 하는 목적이었지만, 어떤 식으로 제휴 서비스를 가능하게 할 것인지는 업체가 자율적으로 고민해야 할 문제이다.

이처럼 연계정보(CI)는 애초에 생성할 필요가 없었다. 오히려 연계정보(CI)는 이용자의 프라이버시 및 개인정보 자기결정권을 위협할 수 있다. 연계정보(CI)는 주민등록번호와 달리 번호 자체에 개인정보를 포함하는 것은 아니지만, 범용적으로 활용되는 개인식별자라는 점에서 주민등록번호의 문제점을 그대로 갖고 있다. 또한 완전히 별개의 고유식별자도 아니고 주민등록번호와 1:1 매칭되는 식별자이기 때문에, 주민등록번호와 연계될 수도 있다. 연계정보(CI)가 그 편리함 때문에 서로 다른 사업자에 의해 활용된다면, 정확하게 그만큼 연계정보(CI)는 범용 식별자로서 위험성을 갖고 있는 것이다. 아이러니하게도 정부가 운영하고 있는 <e-프라이버시 클린 서비스>[21]가 이러한 위험성을 보여준다. 이 서비스를 통해 이용자들은 자신이 어떤 사이트에서 본인확인을 했는지 그 내역을 조회할 수 있고 탈퇴할 수도 있다. 내가 어떤 사이트에 가입되어 있는지는 내 관심사와 취향을 알 수 있는 매우 민감한 정보다. 이처럼 민감한 정보들이 데이터베이스화되어 있다면 언제든지 유출될 위험이 있을 뿐만 아니라, 더 큰 문제는 정부가 언제든 나의 사이트 가입

21) e프라이버시 클린서비스 https://www.eprivacy.go.kr/

내역을 확인할 수 있다는 것이다. 물론 영장이 있어야 하겠지만 그러한 정보를 파악할 수 있는 물리적 조건이 마련되어 있다는 것 자체가 위협이 아닐 수 없다.

더 큰 문제는 이처럼 주민등록번호와 매칭되어 개인을 고유하게 식별할 수 있는 식별자임에도 불구하고 연계정보(CI)는 법적 근거가 없다는 것이다. 회원번호와 같이 개별 사업체가 자율적으로 고객을 관리하기 위한 식별자라면 모르겠지만, 연계정보(CI)는 주민등록번호에 기반하여 생성되며 우리나라 국민 모두에게 자신의 의사와 무관하게 부여되기 때문에 당연히 법적 근거를 가져야 마땅할 것이다. 현재 연계정보(CI)는 방송통신위원회 고시인 「본인확인기관 지정 등에 관한 기준」 제2조(정의)에 규정되어 있을 뿐이다. 현재와 같이 필요성도 법적 근거도 없이 연계정보(CI)를 활용하는 것은 위헌적이다.

그러나 연계정보(CI)는 폐기되기는커녕, 오히려 그 사용이 더 활성화되려 하고 있다. 2019년 2월, 과학기술정보통신부는 ICT 규제 샌드박스의 일환으로 KT와 카카오의 'CI를 이용한 모바일 전자고지' 사업을 임시허가하였다.[22] 여권 만료 안내, 예비군 훈련 통지 등 공공기관이 전자고지를 우편이 아니라 카카오톡이나 문자메시지로 하겠다는 것이다. 이를 위해 공공기관이 보유하고 있는 주민등록번호를 연계정보(CI)로 일괄 변환할 수 있도록 해달라는 것이 규제 샌드박스 신청의 요지다. 사실 공공기관이 원하는 사람에 한해 동의를 받고 카카오톡 계정이나 휴대전화 번호를 수집하면 가능한 서비스다. 연계정보(CI)를 활용하면 더 간편하고 더 적은 비용으로 가능할 것이다. 원래 전체주의적 시스템이 더 효율적이지 않은가.

22) 한겨레, "모바일 전자고지 '본인 동의 없는 본인확인' 논란", 2019. 3. 4.

5. 결론

한편에서는 한국의 개인정보보호법이 지나치게 강하다고 하지만, 한국에는 아직 개인정보 보호원칙에 맞지 않는 법률과 관행이 너무 많다. 주민등록번호, 휴대전화 실명제, 연계정보(CI) 등이 모두 그렇다. 주민등록번호는 수집 목적이 명확해야 하고 그 목적 내에서만 활용해야 한다는 원칙에서 벗어난다. 휴대전화 본인확인 역시 휴대전화 서비스의 제공에 필수적인 것은 아니다. 연계정보(CI) 또한 애초에 존재할 필요가 없는 번호이다. 본인확인과 관계없이 단지 서로 다른 서비스 업체들의 편의를 위해 만들어진 것이기 때문이다. 정보주체에게는 내 연계정보(CI)를 제공하지 않을 권리조차 보장되지 않는다. 더구나 이 세 가지 제도 모두 개인정보의 근간이 되는 주요 식별자와 관련된다. 그만큼 개인의 프라이버시와 개인정보 자기결정권에 미치는 영향이 지대하다.

물론 이러한 시스템이 존재하지 않거나 상대적으로 약한 다른 나라라고 하여 개인에 대한 촘촘한 감시가 없는 것은 아니다. 본인확인을 하지 않더라도 온라인 개인정보의 흔적들을 모아 쉽게 개인을 추적할 수 있다. 특히 소수의 공룡 IT 기업들에 의한 개인정보 독점 문제도 심각하다. 그러나 오히려 개인에 대한 추적과 감시가 쉬워지는 환경으로 변화하고 있기 때문에라도, 기존의 본인확인을 강제하는 시스템에서 하루빨리 탈피할 필요가 있다. 단지 전환에 드는 비용 때문에 이런 구시대적 시스템을 유지하겠다는 것은 한국 사회에서 개인정보보호는 포기하겠다는 선언이나 다름없기 때문이다.

02 데이터 기반 선거와 프라이버시

김유향 국장 (국회입법조사처)

1. 들어가며

데이터 과학의 발전과 더불어 데이터 기반의 맞춤형 선거전략의 중요성이 커지고 있다. 데이터 기반 선거의 대표적인 예는 2012년 11월 미국 대통령 선거에서의 버락 오바마 대통령의 선거전략이다. 2008년 이른바 소셜미디어 선거를 통해 승리하였던 오바마 대통령은 2012년에는 당시 발전하고 있던 빅데이터를 활용해 선거에서 압도적으로 승리하였다. 이후 각종 데이터 기반 타겟팅 선거전략이 발전하고 선거에의 영향이 입증되면서 선거에서 데이터 활용도 더욱 확대되었으며, 더불어 전통적인 선거여론조사보다 훨씬 정확하게 선거 결과를 예측한 미국의 데이터학자 네이트 실버(Nate Silver)의 활약 등에 힘입어 이른바 데이터 기반 선거와 정치의 시대가 도래되었다고 할 수 있다.

그러나 데이터를 활용한 선거의 효용성이 커지면서 그만큼 요구도 늘어나고 데이터의 이용행태와 프라이버시 침해 그리고 나아가 여론조작 등의 문제가 새로운 문제로 부상하고 있다. 대표적인 사건이 케임브리지 애널리티카(Cambridge Analytica) 사건으로서 이 사건은 이용자의 개인정보를 판매하여 개인정보와 프라이버시를 침해한데서 나아가 데이터가 실제 선거의 승패를 좌우하는데 악용될 수 도 있으며, 데이터 맞춤형 선거 및 정치전략이 결국 현대 민주주의에 위기가 되고 있음을 보여준 사례였다.

이 글에서는 데이터 기반 선거의 대표적 사례인 2012년 미국 대선과 오바마의 선거전략, 그리고 케임브리지 애널리티카 사건과 2016 미국 대선을 중심으로 데이터 기반 선거의 특징, 데이터 기반 선거에서의 개인정보 침해 및 프라이버시의 문제점을 서술하고 그 의미를 분석하고자 한다.

2. 빅데이터 시대 선거

2000년대 들어 급격히 발전하던 IT와 데이터처리 기술을 가장 적극적으로 선거에 활용하기 시작한 국가는 미국이었다. 2008년 당시 가장 주목받았던 서비스인 소셜미디어를 선거전에 적극적으로 활용해 젊은 세대와 흑인층 등 정치무관심층을 동원하고 선거에 승리하였던 오바마는 2012년에는 새로운 도전에 직면하였다. 즉 소셜미디어는 이제 일상이 되었고, 상대진영도 적극 활용하고 있었으며, 경제적 위기는 지속되어 선거에 대한 부정적 인식은 개선되지 않았다. 2008년 선거는 소셜미디어 선거였고 오바마 선거대책본부는 정식 IT팀이 없었으며, 페이스북의 크리스 휴즈 등 다수의 전문가들이 참여했지만, 전체적으로 외부기업의 제품들에 크게 의존하는 방식을 취하였다. 독자적인 유권자투표촉진시스템 Houdini를 운영했지만, 전국에서 전달된 데이터(등록된 유권자 코드)를 모아, 활용하고 해석하는 것까지는 기술이 진화하지 못하였다.

이러한 상황에서 오바마 캠프가 주목하고 활용하였던 것이 데이터 기반 선거였다. 2012년 선거에서는 이전의 소셜미디어와 모바일 동원전략은 계승하되, 내부에 정식 기술개발·운용팀을 발족해서 데이터 기반 선거시스템을 구축하고, 대선 2년전에는 'Narwhal[1]'과 'Dreamcatcher'[2]라는 이용자 데이터 기반 프로젝트를 가동하기 위해 캠프에 빅데이터 분석팀을 설치하였다. 특히 Narwhal 시스템은 현장에서 움직이는 자원봉사자(모바

1) 북극해에 사는 고래의 일종을 의미하며, 다양한 정보출처로부터 수집한 데이터를 실시간 종합, 동기화하는 시스템.

2) 웹상의 유권자에 대한 마이크로 타겟팅을 실시하는 시스템.

일, 전화 등), 「팀디지털」(웹이나 소셜미디어 담당), 「팀데이터」(빅 데이터 해석을 담당)로 구성되어 있으며, 여기서 모아지고 분석된 데이터에 기반하여 오바마 캠프의 선거전략이 만들어지고 실제 선거운동이 이루어졌다.

선거와 관련한 빅데이터 분석유형 중에서 가장 기본적인 것으로는 선거결과를 예측하기 위한 통계학적 빅데이터 분석과 상품판매 데이터를 활용한 선거예측방법, 빅데이터 여론조사 방법 등이 있다. 통계학적 빅데이터 분석은 통계전문가 네이트 실버에 의해 주도된 것으로 기존 선거관련 데이터를 광범위하게 수집하여 그들 간의 관계를 찾아내는 것을 통해 선거결과를 예측하는 것이다. 또한 상품판매 데이터를 이용한 선거예측 및 상품소비와 정치성향의 관계분석 등도 많이 활용되는 분석유형이며, Netapp은 대선후보 이름이 적힌 편의점 커피컵 판매량 및 할로윈용품 가게에서 판매된 후보얼굴의 마스크 판매량 등을 통해 대선결과를 예측하는 도구이다.

데이터 활용이라는 2012년의 IT 환경 변화를 배경으로 오바마 선거에서 등장한 주목할 데이터 기반 전략으로 마이크로 타겟팅(Micro-target)을 들 수 있다. 선거에서 마이크로 타겟팅이란 유권자 개인별 특성을 파악하여 그에 맞는 개인맞춤형 선거운동을 펼치는 것을 의미하는데 이 전략을 사용하기 위해서는 첫 단계에는, 전제 조건으로 데이터 수집과 데이터베이스 구축을 해야 한다. 빅데이터는 주로 사람들이 많이 이용하는 트위터와 페이스북의 글을 통해서 사람들의 성향을 분석하고, 개인별 정보를 축적할 수 있다. 둘째 단계에서는 구축된 통합 데이터베이스를 대상으로 군집분석을 하여, 거주지 특성, 소비형태, 라이프 스타일과 취미성향, 가족 형태, 미디어 이용 행태 등이 서로 비슷한 사람들끼리 하나의 그룹으로 묶는 것으로 수십 개, 많게는 수백 개의 특성화 그룹으로 분류할 수 있다. 이어 세 번째 단계에는 그룹별로 특정 후보에 대한 정치적 선호도를 예측하는 연관성분석을 하고, 네 번째 단계는 각 그룹별로 관심 이슈가 무엇인지 분석하는 관심이슈를 추출하여, 타겟에 맞는 전략을 구사한다.

오바마 후보 캠프는 TV 등 전통 미디어와 기존의 여론조사, 정치평론가 등 전문가의 판

단에 의존하지 않으며 철저한 데이터 분석에 기초한 데이터 기반 선거전략을 채택함으로써, 선거운동의 새로운 패러다임을 형성하였다. 이때 만들어진 빅데이터 분석팀은 SNS에서 확보한 데이터, 구매가능한 모든 상업용 데이터와 공공데이터 및 실무자가 직접 발로 뛰며 수집한 정보들까지 모두 취합하여 거대한 데이터베이스로 만들었으며 이를 기반으로 선거전략을 도출하였다. 흩어져있던 지지자 리스트 등 데이터를 모으고 통합해서 실제 선거에 활용할 수 있는 데이터로 만들고 빅데이터를 이용해 확보한 정보들을 이용해 각각 개별 유권자들의 니즈에 맞는 적절한 솔루션을 개발해 마이크로 타켓팅 기법으로 적극 활용하였다.

또한 빅데이터 분석팀은 유권자 개개인의 성향과 특정 정당 및 후보에 대한 선호도를 파악하여 유권자를 5가지 성향으로 나누고 이들을 공화당과 롬니 지지자, 민주당과 오바마 지지자, 그리고 부동층으로 분류하여 이들에 대한 개인적 성향파악에 집중하는 선거 전략을 수립하였다. 이에 기반을 두어 자기편의 가능성이 있는 대상을 설득하는 데 힘을 기울이는 데이터 마이닝을 활용해 잠재적 지지자를 세밀하게 타겟팅하는데 성공하였다.

데이터 마이닝을 활용한 타겟팅 전략은 오바마의 선거전략 전반을 관통하는 것으로 후원금을 모금하고, 투표를 권유하는 등의 운동에 적용되었다. 예를 들면 후원금 모금을 계획할 때는 "캘리포니아주 거주 40~49세의 여성을 선거자금모금 파티에 초대하려고 할 때, 가장 영향력있는 셀럽은 누구인가"라는 질문에 대한 데이터 해석 결과, 조지 클루니가 선택되어 클루니 자택에서 오바마 대통령도 참가한 파티를 개최하였다. 이 데이터 해석 결과는 성공적으로 1인당 4만달러짜리 고액권이 불티나게 팔려 하룻밤에 1,500만 달러의 후원금을 모으는 대성공을 거두었으며, 이를 그대로 적용하여 뉴욕에서는 사라 제시카 파커, 오하이오에선 브루스 스프링스틴 등 셀럽의 활용도 지역 특성에 맞게 세밀하게 분석하여 선정하였다. 후원금 모금 파티는 미국 선거에서 매우 흔한 방식이지만, 과거와 다른 점은 데이터 해석에 기반해 후원금 모금의 효과를 더 높였다는 점에서 차이가 있다.

또한 투표권유 방식 또한 데이터 마이닝을 통해 타겟 맞춤형의 발신자 선정 및 메시지 전

달을 시도하였고, 데이터 분석에 기반한 인플루언서 활용 또한 투표권유에 크게 기여하였다. 특히 유권자의 정치헌금 기부명단, 각종 면허, 소유차량, 구독신문, 신용카드 정보, 선호 브랜드, SNS 활동 내용에 관한 정보를 수집하여 유권자의 성향을 파악하고, 분석된 유권자 성향 자료를 바탕으로 마이크로 타겟 방식의 철저한 맞춤형 선거운동을 통해 부동층을 움직여서 재선에 성공하였다. 오바마 캠프의 데이터 분석팀은 수치에 기반한 고도의 선거전략을 수립했고, 캠프의 모든 중요한 사안은 소수의 경험과 직감에 의존하지 않고 데이터 분석에 기반하여 결정을 내렸다.

물론 당시 공화당의 미트 롬니 후보도 예비선거 7개월 전 빅데이터 분석팀을 출범시켰으며 이 분석팀을 중심으로 ORCA프로젝트를 전개하였으나, 2008년부터 축적된 오바마 캠프의 데이터와는 양과 질에서의 차이가 있었기에 시스템 구축과 활용에 많은 문제점을 노출하고 실제 선거에 큰 도움을 주지 못한 것으로 평가된다. 이처럼 미국 대선에서 빅데이터를 활용한 오바마의 승리이후 데이터 기반 선거전략은 공화당은 물론 전 세계적으로 확산되었고, 지금은 이를 빼고는 선거전략을 논할 수 없을 정도로까지 인식되고 있다.

3. 데이터 기반 선거와 프라이버시

2012년 미국 대선이후 IT발전과 데이터 기반 선거전략의 활용은 2016년 미국 대선과 트럼프 등장에 다른 의미의 기여를 하였다. 2012년 선거에서 시민들의 의사를 파악하고 그에 맞는 정책을 구축하기 위한 전략으로 인식되어온 데이터 기반 선거전략은 개인정보를 남용하고 프라이버시를 침해하여 선거결과를 왜곡시킬 수 있음을 보여주었다. 이를 극명하게 보여준 사례가 케임브리지 애널리티카와 2016년 트럼프 대통령의 등장이며 여기서는 케임브리지 애널리티카 사건을 중심으로 논의를 정리하고 평가하고자 한다.[3] 2012년

3) 이하에서는 Christopher Wylie, Mindf*ck : Inside Cambridge Analytica's Plot to Break the World, Profile Books, 2019.10.8.; Brittany Kaiser, Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again, HarperCollins, 2019. 참조.

오바마의 선거전략과 2016년 트럼프 캠프의 차이점은 트럼프 진영은 빅데이터 심리분석에 더해, 미결정 유권자들에게 심리분석을 기반으로 마이크로 타겟팅 광고를 보내 결과를 유리한 방향으로 유도하였다는 것이다.

오바마가 2012년 빅데이터와 데이터마이닝기법 등을 활용하여 선거에서 승리하면서 소셜미디어 시대 개인이 생산하는 정보와 캠페인 테크(Campaign Tech)의 결합은 선거전략에서 가장 중요하게 고려하는 요인이 되었다. 그러나 데이터 기반 선거전략과 정치과정에서의 상시적 데이터 활용은 긍정적 측면과 더불어 많은 문제점도 내포하고 있다. 먼저 "빅데이터 분석은 인관관계가 아닌 상관관계를 나타낸 것으로서" 정확한 예측보다 경향성을 확인할 때 유용한 것이므로 결과에 대한 과대평가로 잘못된 판단 및 전략이 도출될 가능성이 여전히 크다는 것이다. 즉 데이터 기반의 전략은 아직은 발전 과정에 있기에 이용에 한계가 있다는 지적도 많다.

그러나 무엇보다 큰 문제점은 대량의 개인정보를 수집하고 관리하는 과정에 개인정보 유출과 프라이버시 침해 가능성이 항상 존재한다는 것이다. 케임브리지 애널리티카 사건이 대표적인 것으로 페이스북 이용자를 대상으로 '심리검사퀴즈 앱(ThisIsYourDigitalLife)'을 운영하는 글로벌 사이언스 리서치(GSR, Global Science Research)는 이 앱을 페이스북과 연동하여 27만 명의 페이스북 이용자를 모집하고 이들의 친구목록을 통해 약 5천만 명의 개인정보를 수집하였고, 수집한 개인정보를 케임브리지 애널리티카에 제공하였다. 이 앱이 동의를 얻은 이용자는 27만명이었지만, 페이스북의 오픈 그래프 API를 통해 이들의 친구정보까지 접근하면서 약 5천만명에 이르는 이용자정보를 가져올 수 있었다. 캠브리지 애널리티카는 글로벌 사이언스 리서치에게서 받은 페이스북의 사용자 프로필 데이터를 영국의 EU탈퇴 투표와 2016년 미국 대선 당시 도널드 트럼프 후보의 선거 운동에 활용하였다. 이는 실제 트럼프의 승리에 기여한 것으로 평가되고 있다.[4] 트럼프 당선

4) 내부고발자인 크리스토퍼 와일리(Christopher Wylie)가 2016년 미 대선 당시 트럼프 캠프에 페이스북 이용자 프로필 분석 데이터를 전달한 사실을 2018년 3월 뉴욕타임즈와 가디언에 폭로하면서 세계 각국에서 개인정보유출을 둘러싼 논란이 야기되었다.

이나 EU 이탈의 다수파 형성을 성공시킨 것으로 되어있다. 이로써 Facebook 등 거대 플랫폼 기업의 개인정보 관리와 비즈니스 모델의 문제점이 사회적으로 주목받았고 마크 저커버그가 미 의회에서 증언하기도 하였다.

빅데이터는 그 수집·활용을 위해 개인의 인적사항, 개인이 온라인상에서 작성한 글, 소비내역, 위치정보 등 개인식별정보(personal identifiable information, PII)가 포함될 수 있다.[5] 2012년 연구에 따르면 페이스북의 '좋아요' 버튼 결과를 68개 분석하면 사용자의 프로필을 대략 알 수 있으며, '좋아요' 버튼 150개, 300개로 겹쳐 분석할 경우 학력, 지능, 종교, 술과 담배를 좋아하는지 등에 이르기까지 파악할 수 있다고 한다. 케임브리지 애널리티카의 작업은 기본적으로 성격 프로파일을 기반으로 한 투표행동분석이다. '개방성(open)', '성실성(Conscientious)', '외향성(Extroverted)', '우호성(Agreeable)' '신경성(Neurotic)정신적 안정' 등 5가지 요소로 사람들의 성격을 분류하는 Five-Factor Model (OCEAN)을 바탕으로 32개의 주요 성격그룹으로 나누어 인간의 심리, 성격을 수치화하였다. 케임브리지 애널리티카는 페이스북에서 수집한 사람들의 데이터를 이 분류에 따라 분류하고 국민투표에서 '설득가능한 유권자(Persuadable)'를 추출하고, 페이스북의 마이크로 타겟팅 광고를 사용하여 설득가능한 유권자의 투표 행동을 변화하도록 시도했다. 미국의 복잡한 선거구와 선거인단 제도로 인해 매우 중요한 부동표를 움직이는 데 성공하여 트럼프를 당선시키고, EU탈퇴 결정을 이끌어낸 것으로 평가된다.

마이크로 타겟팅 자체는 일반적 마케팅에서 사용하는 수법이다. 특히 광고의 세계는 빅데이터와 소비행동 예측에 기반하여 움직인다. 빅데이터는 데이터의 양이 많을수록 적중률이 높아지는데, 현금 이용이 줄어들고 소비활동이 인터넷 상거래, 신용카드로 이루어지

5) 실제 빅데이터의 활용에 대해서는 국가 간 정책에서 차이가 있다. 미국은 시민의 알 권리와 기업의 활동을 강조하고 있기에, 개인정보를 활용한 빅데이터 분석이 활발하게 진행되고 있으며, 반면 유럽은 개인정보보호를 보다 엄격하게 보장하고 있다.

면서 소비자 행동을 추적하기는 더욱 쉬워졌다. 소비자 행동을 예측하고 타겟팅하는 방법은 유권자 행동을 예측하고 타겟팅하는 데 이용되었다. 케임브리지 애널리티카는 이를 심리조작과 선전에 이용했다. 또한 진실 또는 허위정보를 막론하고 상대 후보를 비방하는 수많은 메시지를 소셜미디어에 유포하고 그것이 어떻게 수용되는지를 시험했다. 이러한 마이크로 타겟팅에는 대량의 개인 프로파일링 자료가 필요했으며, 케임브리지 애널리티카가 이용한 것은 Facebook의 데이터로 2014년 8월까지 취득한 사용자 정보 수는 미국을 중심으로 약 8,700만 사용자에 달했다.

문제는 이러한 정보를 심리 조작 도구 (psychological mindfuck tool)로 활용하여 선거와 정치의 결과를 원하는 방향으로 유도하는 것이다. 여론에 영향을 미치도록 많은 양의 정보를 이용하여 정치의 풍향을 바꿔버리는 시도는 실제 케임브리지 애널리티카를 통해 영국의 브렉시트 투표와 2016년 미국 대통령 선거에서 이루어졌다. 케임브리지 애널리티카는 미국과 영국의 선거 이전에 트리니다드 토바고, 케냐, 나이지리아 등 국가에서 선거결과에 영향을 줄 수 있는 실험을 진행하였고 이후 영국과 미국의 중요한 선거에서 대규모 선거광고 작업을 진행하였다.

Facebook과 같은 거대 플랫폼 기업의 수익모델은 이용자의 정보를 가능한 많이 수집하여 그 행동을 분석할 수 있도록 설계되어 있다. 특히 페이스북의 개인에 최적화된 타임라인은 사용자의 플랫폼내 체류 시간이 길수록 더 많은 광고료가 생긴다. 따라서 페이스북 등 소셜플랫폼 기업은 사용자의 정보를 가능한 많이 수집하여 그 행동을 분석할 수 있도록 설계되고, 이른바 '사용자 참여'라는 이름아래 수집된 개인 데이터는 정치적 선전을 위한 좋은 재료가 된다. 케임브리지 애널리티카가 페이스북 사용자의 개인정보를 수집하고 사용자의 친구에 대한 정보를 얻을 수 있었던 것은 페이스북의 Graph API의 설계와 기능에 의한 것으로 이 기능은 인터넷 상의 다양한 요소를 페이스북의 생태계 속에 묶어두는 것이 가능하게 하였다. 페이스북의 페이지나 사용자 계정은 고유의 ID가 있으며, 정보를 얻기 위해 해당 ID를 직접 쿼리 할 수 있다. 공공기관, 기업 등에게는 페이스북 사용자의 활동, 연결, 감정 상태에 대한 액세스 및 고급 검색 기능을 제공하였다. Graph API는

사람과 그의 선호, 연결, 장소, 위치 업데이트, 이력 등을 경제적으로 활용 가능한 데이터로 만들어주었다.

미국 연방거래위원회(FTC)는 2019년 7월 케임브리지 애널리티카를 둘러싼 개인정보 유출문제에서 페이스북에 50억달러의 벌금을 부과했다. 거대 플랫폼 기업들은 방대하게 구축한 이용자 데이터를 기반으로 수익을 창출하기에 사실상 이용자 개인정보보호에 둔감할 수 있다. 케임브리지 애널리티카 사건은 개인의 정체성과 행동양식 데이터가 거래되면서 단순히 상업적 이익만이 아닌 민주주의를 근저에서부터 흔들 수도 있다는 것이다.

4. 민주사회에의 도전과 과제

거미줄같이 연결된 소셜 네트워킹의 시대, 진짜 같은 가짜를 만들어내는 딥페이크(deep fake) 시대, 첨단 AI와 ICT 발전의 시대에 인간은 더 똑똑하면서 자유로워지고, 사회는 민주주의의 이상에 성큼 다가가고, 세계는 좀 더 가까워져서 서로를 더 잘 이해하게 될 것이라는 기대가 무너져가고 있다. 2016년 미국 대선과 영국의 브렉시트 투표는 정치적 사건이지만, ICT 발전이 개인과 사회의 민주주의에 미치는 영향을 가장 극명하게 보여준 전후 시대의 한 획을 그은 사건이었다.[6)]

2012년 오바마의 선거전략은 ICT를 활용하여 당시 화석화된 대의민주주의에 새로운 기운을 불어넣을 수 있을 것으로 기대되었다. 다수 국민의 목소리를 듣고 실제 정치과정에 반영하는 이상적 민주주의의 모델은 현대 대중사회에서는 국민의 의사를 효과적으로 모으는 기술, 민의를 수집·반영하는 기술의 한계에 의해 효과적으로 작동하지 못하였다. 오바마 선거전략은 데이터 기반 기술을 통해 많은 국민의 의사를 효과적으로 모아서 정책에 반영할 수 있는 수단으로 주목받았다. 데이터 기반 전략을 활용하면 어떤 문제에 대해서, 어떠한 해결책을 제안하면, 어떤 그룹의 사람이 어느 정도 지지하는지 등의 시뮬레이

6) 김유향, “탈진실 시대에 팩트를 논하다”, KISO저널 제36호, 2019.9.30.

션을 실시하는 것이 가능하였기 때문이다. 소셜미디어나 빅데이터, 혹은 최근 다양하게 등장하고 있는 새로운 정보기술을 잘 사용하면, 보다 효율적으로, 여론의 방향성을 보다 정확하게 파악하고, 그 효과를 보다 정확하게 예측해, 보다 많은 사람이 바라는 정책을 실행할 수 있게 될지도 모른다.

그러나 이러한 낙관주의는 개인정보와 프라이버시 침해라는 대가가 따르는 것이었다. 데이터 기반 선거는 기술의 활용으로 인한 캠페인 방식의 다양화, 유권자의 선호에 부합하는 공약 등 선거전략 구축 등의 장점을 넘어 개개인의 프라이버시를 침해하고, 특정 후보자에게 유리한 여론을 만들어 냄으로써 실제 민주적 정치과정의 꽃인 선거가 공정하고 원활하게 작동하는 것을 방해하는 강력한 수단이 되고 있다.

KOREA LEGISLATION RESEARCH INSTITUTE

KLRI

III

한국 사회와 데이터 프라이버시의 위기

01 개인정보보호법 붕괴작전
신용정보법의 개정은 무엇을 위한 것인가

김보라미 변호사 (법무법인 디케)

1. 개인정보 3법의 개정 과정과 「신용정보의 이용 및 보호에 관한 법률」

(1) 배경

'개인정보 3법', 즉 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'), 「신용정보의 이용 및 보호에 관한 법률」(이하 '신용정보법'), 「개인정보 보호법」(이하 '개인정보보호법')이 2020년 1월 9일 개정되었다. 개인정보 3법의 개정의 원동력은, "개인정보"라는 성격보다는 "데이터"라는 성격을 강조한 정부·여당의 접근방법에 근거한 것이었다. 개인정보 3법을 "데이터 3법"으로, 그리고 데이터 3법의 규제완화(정보주체의 동의 없는 활용의 확대)를 "데이터경제육성의 비책"으로 홍보하였다.

문재인 대통령은 2018년 8월 31일 '데이터경제 활성화 규제혁신 행사'에 참석해 "4차 산업혁명시대, 미래 사업의 원유가 바로 데이터"라고 칭하며 "데이터를 잘 가공·활용하면 생산성이 높아지고 새로운 서비스와 일자리가 생겨난다"며, 데이터 규제 혁신이 혁신성장과 직결된다고 강조했다.[1] 그러나 대통령은 데이터 규제혁신만을 강조한 것이 아니

1) MBC, "문 대통령 '4차 산업혁명 시대의 원유는 데이터…1조원 투자'", 2018. 8. 31. https://imnews.imbc.com/news/2018/politics/article/4796495_30795.html (최종방문일 2020. 8. 10.)

라, "개인정보보호의 중요성 등을 감안해 개인과 관련한 정보를 개인정보, 가명정보, 익명정보로 구분해 개인정보는 철저히 보호하고, 가명정보는 확실한 안전장치 담보 후 활용하며, 익명정보는 규제 대상에서 제외해 자유롭게 활용하게 하자"라고도 제안하였다. 대통령의 개인과 관련한 정보를 개인정보, 가명정보, 익명정보로 구분한 제안은 2018년 4월 5일 4차산업혁명위원회 제3차 규제·제도 혁신 해커톤의 토론결과[2]에 기반한 것이다.

(2) 해커톤에서의 신용정보법 개정방향

개인정보 3법의 개정 단초가 된 "개인정보의 보호와 활용의 균형"에 대한 2차례에 걸친 해커톤에서는 다음과 같은 논의가 진행되었다.

우선, 2018년 2월 1일부터 2월 2일까지 이루어진 4차산업혁명위원회 해커톤에서는 다음과 같이 합의가 이루어졌다. 이 논의에서는 유럽연합의 개인정보보호법(GDPR)을 참고하여 개인정보, 가명정보, 익명정보로 구분하되 나머지 구체적 합의는 차후 회의에서 다시 진행하기로 하였다.

① 개인정보 관련 법적 개념체계 정비

- 개인정보와 관련된 법적 개념체계는 개인정보, 가명정보, 익명정보로 구분하여 정비하기로 하였다. 그리고 익명정보는 개인정보보호법의 적용대상이 아니라고 합의하여 개인정보와 구분하였다.

② 익명정보 개념은 법에 명시하지 않음

- '익명정보' 개념을 명확히 하기 위하여 '익명정보' 정의를 법에 명시하는 대신 EU GDPR 전문(26)을 참조하여 '개인정보'의 개념을 보완하기로 논의하였다.

2) 4차산업혁명위원회 보도자료, "가명정보의 활용 범위와 목적 등에 대한 합의, 클라우드 이용 활성화를 위한 정보등급 체계 개편, 드론산업 발전을 위한 업계의 애로 해소 방안 논의 - 4차산업혁명위, 제3차 규제·제도혁신 해커톤 개최 -", 2018. 4. 5. 참조.

③ '가명정보'에 대한 법적 근거 마련
- '가명정보'의 정의 및 활용에 관한 법적 근거를 마련하기로 하였다.

④ 개인정보의 보호와 활용에 대한 지속적 논의 진행
- 개인정보의 보호와 활용에 관한 주요 이슈들에 대해서 추가적인 논의를 진행하기로 하였다.[3)]

이후 2018년 4월경 4차산업혁명위원회에서 개인정보의 보호와 활용에 대한 해커톤을 앞두고 시민사회로부터 "개인정보보호위원회의 강화 및 보호체계의 개선"의 요청이 강하게 대두되자, 최초 1차 해커톤에 참석하지 않았던 금융위원회도 신용정보법의 체계개선 때문에 함께 참석하게 되었다.

2018년 4월 초에 진행된 2차 해커톤 당시 개인정보체계 및 거버넌스에 대해서는 밤새도록 금융위원회가 동의하지 않아 끝내 합의에 이르지 못했다. 그러나 결국 마지막 날 개인정보 거버넌스의 강화 및 통일화가 국정운영 5개년 계획 내에 포함되어 있는 100대 과제 중 하나임을 언급하자 그제서야 이 부분에 대하여 애매한 논지(각 부분에서 고유하게 규정할 필요가 있는 사항에 대한 예외)로 합의가 이루어졌다. 당초 위 개인정보 거버넌스의 강화 및 통일화는 2018년부터 도입하기로 한 공약으로 개인정보보호 측면에서 국민인권을 우선하는 민주주의의 회복과 강화 전략에서 도입된 내용이었으며, 이를 통해 개인정보보호 체계의 효율화를 도모하고자 한 것이었다.

◎ 정보통신망법, 신용정보법, 위치정보법은 각 부문에서 고유하게 규정할 필요가 있는 사항을 제외하고, 개인정보보호와 관련한 중복, 유사 조항에 대해서는 통일적 규율이 필요하다는 점을 합의하였다.

◎ 그리고, 개인정보보호와 활용을 위한 거버넌스 개선방안이 마련되어야 한다는 점에 동의하였다.[4)]

3) 4차산업혁명위원회 보도자료, "개인정보 관련 법적 개념 체계 정비 합의, 전자서명법 개정을 통한 다양한 전자서명 활성화 방안 논의" - 4차산업혁명위, 제2차 규제 · 제도혁신 해커톤 개최 -, 2018. 2. 5., 3면.

4) 4차산업혁명위원회 보도자료, "가명정보의 활용 범위와 목적 등에 대한 합의, 클라우드 이용 활성화를 위한 정보등급 체계 개편, 드론산업 발전을 위한 업계의 애로 해소 방안 논의" - 4차산업혁명위, 제3차 규제 · 제도혁신 해커톤 개최 -, 2018. 4. 6., 4면.

즉, 금융위원회에서는 개인정보보호 거버넌스에서 중요한 역할을 할 의지를 계속 피력하였고, 이 과정에서 해커톤에서 합의에 이른 부분은 각 법률에서 고유하게 규정할 필요가 있는 사항을 제외하고는 개인정보보호와 관련한 중복, 유사 조항에 대하여 통일적 규율을 해야 한다는 것이었다. 그러나 실제 입법된 내용은 전혀 그렇지 아니하였다.

(3) 신용정보법 개정안 발의와 후속입법

2018년 11월 15일 인재근 의원이 발의하여 「개인정보 보호법 일부개정법률안」이, 김병욱 의원이 발의하여 「신용정보의 이용 및 보호에 관한 법률 일부개정법률안」이 발의되었다. 정부·여당은 위와 같이 법안을 발의한 직후인 2018년 11월 21일 '개인정보보호 관련 법안 개정 당정청 회의'를 열고 "데이터완화와 관련한 정보주체(개인)의 권리에 대한 입법은 내년으로 미루면서 개인정보보호위원회 권한 강화와 가명정보 활용 허용을 연내 추진하겠다"라는 결론에 이르렀다.

김병욱 의원이 발의한 신용정보법 개정법률안은 타 의원들이 대표발의한 신용정보법 개정법률안들과 통합되어 2019년 11월 29일 정무위원회안(대안)으로 정무위원회에서 대안가결되었고, 법제사법위원회에서 같은 날 상정되었고, 2020년 1월 9일 법제사법위원회에서 체계·자구 심사를 거쳐 당일 본회의에서 심의처리되었다.
신용정보법은 통과 당시에도 ① 2014년 전 경제인구의 75%[5]가 피해자로 추정되는 대규모 해킹사건의 반성적 고려로 도입된 신용정보회사의 부수적 영리활동 제한도 모두 허용하였고, ② 박근혜 정권 때에도 위험하다는 비판[6]에 도입하지 못하던 '소셜미디어나 이와 유사한 공개된 정보'를 동의 없이 사용할 수 있도록 허용하였으며, ③ 신용정보와 다른 종류의 개인정보 간 결합에 대하여도 금융위원회가 정보주체의 동의를 받지 않고 사용할

5) 금융감독원, "최근 고객정보 유출 관련 현황 및 대응방안", 2014. 1. 19.자 보도자료.

6) 경실련, 진보넷, 함께하는 시민행동, "인권침해 유발하는 '빅데이터 가이드라인'", 2013. 12. 30.

수 있는지 여부를 결정할 권한마저도 내주었다[7]는 측면에서 개인정보보호법을 우회하고 있다는 비판이 제기되었지만 이러한 문제제기는 입법에 전혀 반영되지 못하였다. 오히려 개인정보 3법은 여야의 합의법안으로 신중한 검토 없이 통과되었다.

즉, 신용정보법은 뒤에서도 살펴보듯이 시행령 및 유권해석의 확대해석과 결합되었다. 그 결과 개인정보 보호체계를 근본적으로 우회하는 과대해진 금융위원회의 권한을 한정해야만 하는 문제가 계속 발생하게 된다. 이에 아래에서는 이러한 사정에 대하여 신용정보법 입법의 문제점, 신용정보법 시행령의 문제점, 상행위 거래정보의 시행령상 문제점, 질병정보의 유권해석의 문제로 나누어 살펴보고자 한다.

2. 신용정보법 관련 법률간 정합성의 문제점

(1) 신용정보법과 개인정보보호법의 관계

신용정보법 제3조의2 제1항에 따르면 "신용정보의 이용 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다."라고 정하고 있으며, 같은 법 같은 조 제2항에 따르면 "개인정보의 보호에 관하여 이 법에 특별한 규정이 있는 경우를 제외하고는 「개인정보 보호법」에서 정하는 바에 따른다."라고 정하고 있다.

따라서 위 규정의 취지에 따르면 개인신용정보에 대하여 신용정보법에서 달리 정하고 있다면 신용정보법에 따르고, 신용정보법에 규정이 존재하지 아니할 경우에만 개인정보보호법에서 정하는 바에 따른다고 해석된다.

한편, 개인신용정보는 대부분 개인정보의 한 종류로서, 신용정보법 제2조 제2호에 따르면 "해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보(가목), 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보(나목)"라고 정하고 있으며, 신용정보에 대하여는 신

7) 경실련, "국회는 금융사들의 로비와 금융위의 부처이기주의로 점철된 신용정보법 개정안 강행처리 중단하라", 2019. 11. 29. http://ccej.or.kr/57444 (최종방문일 2020. 8. 10.)

용정보법 제2조 제1호에서 아래의 [표-1]과 같이 상당히 포괄적으로 규정하고 있다. 특히 일반 상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보뿐만 아니라 향후 신용정보법 시행령상에 포괄적으로 규정된 내용 등을 근간으로 일반 상사거래상 형성되는 대부분의 정보는 개인정보보호법이 아니라 신용정보법이 적용될 수 밖에 없는 상황에 처하게 되었다.

그뿐만 아니라 신용정보법상 수범자인 '신용정보제공·이용자'는 "고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자와 그 밖에 이에 준하는 자로서 대통령령으로 정하는 자"로 규정되어 그 범위가 사실상 일반 상거래회사로 해석될 수밖에 없다.

[표-1] 신용정보의 정의 및 유형별 내용과 범위

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "신용정보"란 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보로서 다음 각 목의 정보를 말한다.
   가. 특정 신용정보주체를 식별할 수 있는 정보(나목부터 마목까지의 어느 하나에 해당하는 정보와 결합되는 경우만 신용정보에 해당한다)
   나. 신용정보주체의 거래내용을 판단할 수 있는 정보
   다. 신용정보주체의 신용도를 판단할 수 있는 정보
   라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보
   마. 가목부터 라목까지의 정보 외에 신용정보주체의 신용을 판단할 때 필요한 정보

1의2. 제1호가목의 "특정 신용정보주체를 식별할 수 있는 정보"란 다음 각 목의 정보를 말한다.
   가. 살아 있는 개인에 관한 정보로서 다음 각각의 정보
      1) 성명, 주소, 전화번호 및 그 밖에 이와 유사한 정보로서 대통령령으로 정하는 정보
      2) 법령에 따라 특정 개인을 고유하게 식별할 수 있도록 부여된 정보로서 대통령령으로 정하는 정보(이하 "개인식별번호"라 한다)
      3) 개인의 신체 일부의 특징을 컴퓨터 등 정보처리장치에서 처리할 수 있도록 변환한 문자, 번호, 기호 또는 그 밖에 이와 유사한 정보로서 특정 개인을 식별할 수 있는 정보
      4) 1)부터 3)까지와 유사한 정보로서 대통령령으로 정하는 정보
   나. (생략)

1의3. 제1호나목의 “신용정보주체의 거래내용을 판단할 수 있는 정보”란 다음 각 목의 정보를 말한다.

가. 신용정보제공 · 이용자에게 신용위험이 따르는 거래로서 다음 각각의 거래의 종류, 기간, 금액, 금리, 한도 등에 관한 정보

1) 「은행법」 제2조제7호에 따른 신용공여

2) 「여신전문금융업법」 제2조제3호·제10호 및 제13호에 따른 신용카드, 시설대여 및 할부금융 거래

3) 「자본시장과 금융투자업에 관한 법률」 제34조제2항, 제72조, 제77조의3제4항 및 제342조제1항에 따른 신용공여

4) 1)부터 3)까지와 유사한 거래로서 대통령령으로 정하는 거래

나. 「금융실명거래 및 비밀보장에 관한 법률」 제2조제3호에 따른 금융거래의 종류, 기간, 금액, 금리 등에 관한 정보

다. 「보험업법」 제2조제1호에 따른 보험상품의 종류, 기간, 보험료 등 보험계약에 관한 정보 및 보험금의 청구 및 지급에 관한 정보

라. 「자본시장과 금융투자업에 관한 법률」 제3조에 따른 금융투자상품의 종류, 발행 · 매매 명세, 수수료·보수 등에 관한 정보

마. 「상법」 제46조에 따른 상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보

바. 가목부터 마목까지의 정보와 유사한 정보로서 대통령령으로 정하는 정보

1의4. 제1호다목의 “신용정보주체의 신용도를 판단할 수 있는 정보”란 다음 각 목의 정보를 말한다.

가. 금융거래 등 상거래와 관련하여 발생한 채무의 불이행, 대위변제, 그 밖에 약정한 사항을 이행하지 아니한 사실과 관련된 정보

나. 금융거래 등 상거래와 관련하여 신용질서를 문란하게 하는 행위와 관련된 정보로서 다음 각각의 정보

1) 금융거래 등 상거래에서 다른 사람의 명의를 도용한 사실에 관한 정보

2) 보험사기, 전기통신금융사기를 비롯하여 사기 또는 부정한 방법으로 금융거래 등 상거래를 한 사실에 관한 정보

3) 금융거래 등 상거래의 상대방에게 위조 · 변조하거나 허위인 자료를 제출한 사실에 관한 정보

4) 대출금 등을 다른 목적에 유용(流用)하거나 부정한 방법으로 대출 · 보험계약 등을 체결한 사실에 관한 정보

5) 1)부터 4)까지의 정보와 유사한 정보로서 대통령령으로 정하는 정보

다. 가목 또는 나목에 관한 신용정보주체가 법인인 경우 실제 법인의 경영에 참여하여 법인을 사실상 지배하는 자로서 대통령령으로 정하는 자에 관한 정보

라. 가목부터 다목까지의 정보와 유사한 정보로서 대통령령으로 정하는 정보

1의5. 제1호라목의 "신용정보주체의 신용거래능력을 판단할 수 있는 정보"란 다음 각 목의 정보를 말한다.

가. 개인의 직업·재산 · 채무·소득의 총액 및 납세실적

나. 기업 및 법인의 연혁·목적·영업실태·주식 또는 지분보유 현황 등 기업 및 법인의 개황(槪況), 대표자 및 임원에 관한 사항, 판매명세·수주실적 또는 경영상의 주요 계약 등 사업의 내용, 재무제표(연결재무제표를 작성하는 기업의 경우에는 연결재무제표를 포함한다) 등 재무에 관한 사항과 감사인(「주식회사 등의 외부감사에 관한 법률」 제2조제7호에 따른 감사인을 말한다)의 감사의견 및 납세실적

다. 가목 및 나목의 정보와 유사한 정보로서 대통령령으로 정하는 정보

1의6. 제1호마목의 "가목부터 라목까지의 정보 외에 신용정보주체의 신용을 판단할 때 필요한 정보"란 다음 각 목의 정보를 말한다.

가. 신용정보주체가 받은 법원의 재판, 행정처분 등과 관련된 정보로서 대통령령으로 정하는 정보

나. 신용정보주체의 조세, 국가채권 등과 관련된 정보로서 대통령령으로 정하는 정보

다. 신용정보주체의 채무조정에 관한 정보로서 대통령령으로 정하는 정보

라. 개인의 신용상태를 평가하기 위하여 정보를 처리함으로써 새로이 만들어지는 정보로서 기호, 숫자 등을 사용하여 점수나 등급 등으로 나타낸 정보(이하 "개인신용평점"이라 한다)

마. 기업 및 법인의 신용을 판단하기 위하여 정보를 처리함으로써 새로이 만들어지는 정보로서 기호, 숫자 등을 사용하여 점수나 등급 등으로 표시한 정보(이하 "기업신용등급"이라 한다). 다만, 「자본시장과 금융투자업에 관한 법률」 제9조제26항에 따른 신용등급은 제외한다.

바. 기술(「기술의 이전 및 사업화 촉진에 관한 법률」 제2조제1호에 따른 기술을 말한다. 이하 같다)에 관한 정보

사. 기업 및 법인의 신용을 판단하기 위하여 정보(기업 및 법인의 기술과 관련된 기술성 · 시장성 · 사업성 등을 대통령령으로 정하는 바에 따라 평가한 결과를 포함한다)를 처리함으로써 새로이 만들어지는 정보로서 대통령령으로 정하는 정보(이하 "기술신용정보"라 한다). 다만, 「자본시장과 금융투자업에 관한 법률」 제9조제26항에 따른 신용등급은 제외한다.

아. 그 밖에 제1호의2부터 제1호의5까지의 규정에 따른 정보 및 가목부터 사목까지의 규정에 따른 정보와 유사한 정보로서 대통령령으로 정하는 정보

(2) 개정 신용정보법과 개인정보보호법의 중첩

앞서 본 것과 같이 개정 신용정보법이 다루는 개인신용정보의 범위가 상당히 광범위하여 일반 상거래정보가 모두 포함되는 상황임에도 불구하고, 아래에서 보듯 이번에 개인정보보호법이 새로 도입한 가명처리, 가명정보, 이종간 데이터 결합을 모두 중복하여 신설하여 금융위원회가 시행령 등의 하위입법으로 그 구체적인 내용 등을 개인정보보호법과 달리 정할 수 있도록 하였고, 실제 하위 입법은 그러한 설계로 개인정보보호법과 신용정보법이 서로 충돌되는 결과에 이르렀다. 결국 개인정보보호법은 개정 신용정보법에 의하여 사실상 우회하게 된 것이다.

[표-2] 신설 신용정보법 규정들

1) 추가정보를 사용하지 아니하고는 특정 개인을 알아볼 수 없도록 처리(가명조치)한 개인신용정보로서 가명정보의 개념을 도입하고, 통계작성(시장조사 등 상업적 목적의 통계작성을 포함), 연구(산업적 연구를 포함), 공익적 기록보존 등을 위해서는 가명정보를 신용정보주체의 동의 없이도 이용하거나 제공할 수 있도록 한 조항(제2조제15호 · 제16호 및 제32조제6항제9호의2·제9호의4 신설).
2) 신용정보회사 등에 대하여 가명조치에 사용한 추가정보는 일정한 방법으로 분리하여 보관하도록 하고, 신용정보회사 등은 가명정보를 보호하기 위하여 일정한 기술적 · 물리적 · 관리적 보안대책을 수립·시행하도록 하며, 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 처리를 즉시 중지토록 하고, 특정 개인을 알아볼 수 있게 된 정보를 즉시 삭제토록 하는 등의 의무를 부과하는 조항(제40조의2제1항.제2항 및 제6항부터 제8항).
3) 더 이상 특정 개인을 알아볼 수 없도록 개인신용정보를 처리하는 익명조치에 대해서는 금융위원회가 지정하는 데이터전문기관의 적정성 평가를 거친 경우에는 더 이상 특정 개인을 알아볼 수 없도록 처리된 정보로 추정하는 조항(제2조제17호, 제26조의4, 제40조의2제3항부터 제5항).
4) 신용정보회사 등이 보유하는 정보집합물을 제3자가 보유하는 다른 정보집합물과 결합할 경우에는 데이터전문기관을 통해서만 하도록 하고, 데이터전문기관이 결합된 정보집합물을 해당 신용정보회사 등에게 전달하는 경우에는 가명조치 또는 익명조치가 된 상태로 전달되도록 하는 등 이종(異種) 산업분야 간의 데이터 결합근거 조항(제17조의2, 제26조의4, 제32조제6항제9호의3)

3. 신용정보법 시행령의 법률 정합성의 문제점

신용정보법은 개인정보보호법과 적용범위가 겹치고 있음에도 그 정의 및 적용에 있어서 동일하지 않다. 그런데 개정 신용정보법의 시행과 발맞추어 진행된 신용정보법 시행령(2020. 8. 5. 시행, 대통령령 제30893호) 또한 개인정보보호법 시행령과 조율되지 아니한 채 서로 다른 취지의 입법이 이루어지고 있다.

한편 개인정보보호법 제7조의8 제1호에 따르면 "개인정보의 보호와 관련된 법령의 개선에 관한 사항" 역시 개인정보보호위원회의 소관에 해당되어 신용정보법상 개인정보의 해석은 개인정보보호위원회가 리더십을 갖고 처리해야 법 전체의 정합성의 측면에서도 타당하다. 그럼에도 불구하고 현재까지 개인정보보호위원회는 출범 초기이기 때문에 이 문제를 직접적으로 다루지 못하고 있어 이 문제가 전혀 해결되지 못하고 있다.

아래에서는 각 신용정보법 시행령의 문제를 살펴보고 최근 문제가 된 상행위 거래정보와 질병정보에 대하여 구체적으로 살펴보고자 한다.

(1) 과도한 포괄위임 조항들

신용정보법 시행령상 "그 밖에 이와 유사한 정보로서 금융위원회가 정하여 고시하는 정보" 또는 "그 밖에 법 제00조와 유사한 정보로서 금융위원회가 정하여 고시하는 정보" 또는 "그 밖에 금융위원회가 정하여 고시하는 업무" 또는 "그 밖에 금융위원회가 정하여 고시하는 정보"라고 정한 부분은 수범자의 예측가능성을 침범하여 다시 고시에 포괄위임하는 형태임에도 과도하게 많이 존재하고 있다.

금융위원회의 고시입법권을 인정하는 규정들을 대략적으로 추려봐도 상당한 수에 해당하는바, 우선 당장 삭제하여도 법집행상 문제없는 조항을 언급하면 아래와 같다.

◎ "그 밖에 금융위원회가 정하여 고시하는 업무/정보/기준/자/사항"

- 시행령 제11조 : 제1항 제5호, 제2항 제4호, 제3항 제9호, 제6항 제7호
- 시행령 제11조의2 : 제1항 제7호, 제2항 제10호, 제3항 제3호, 제4항 제5호

- 시행령 제22조의4 : 제7항 제4호, 제8항 제3호, 제10항 제1호 나목 및 제2호 다목
- 시행령 제30조의3 : 제1항 제4호, 제2항 제3호

◎ "그 밖에 (~와 유사한 정보로서) 금융위원회가 정하여 고시하는" 경우의 형태로 포괄위임한 규정들

- 시행령 제2조 : 제1항 제3호, 제4항 제3호, 제7항 제7호
- 시행령 제22조의4 : 제1항 제4호, 제2항 제3호
- 시행령 제29조의2 : 제1항 제2호

(2) 신용정보법 시행령 제11조의2

신용정보법 제11조의2 제2항 제6호, 제4항 제5호, 제5항 제3호, 제6항 제4호, 제7항 제3호는 "신용정보주체 보호 및 건전한 신용질서를 저해할 우려가 없는 업무로서 대통령령으로 정하는 업무"에 한하여 부수업무를 허용하고 있으나 신용정보법 시행령 제11조의2는 이에 대하여 정하면서 금융상품에 대한 광고, 홍보 및 컨설팅업무를 포함한 신용정보주체의 보호와 무관한 행사기획, 신용정보업 관련 연구, 본인인증, 정보가공 후 제3자 제공업무, 연체사실 통지 대행 등의 업무를 이에 포함시키고 있다.
그러나 우선 위와 같이 제한없는 광고, 홍보 등의 업무를 신용정보주체 보호의 범주로 해석할 수 없을 뿐만 아니라, 과거 여러 차례 발생한 에스케이브로드밴드 개인정보 판매사건 및 홈플러스 개인정보 판매사건과 유사한 사건들을 발생시킬 심각한 위험에 신용정보주체를 노출시키고 있다. 따라서 위 직·간접 마케팅 목적의 업무는 "신용정보주체 보호"라는 명목으로 허용될 수 없다.

그 이외에도 제11조의2가 정하는 대부분의 내용들은 "신용정보주체 보호"와 무관하고 "신용정보업"의 편익을 위한 내용으로 구성되어 있어 대통령령이 정한 "신용정보주체 보호"라는 한계를 일탈한 것으로 해석되는바, 해당 시행령은 전부가 위법적인 문제가 존재한다.

(3) 신용정보법 시행령 제13조 제6호

신용정보법 제15조 제2항 제2호 다목은 "신용정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 정보. 이 경우 대통령령으로 정하는 바에 따라 해당 신용정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내로 한정한다."라고 정하고 있는바, 이는 대법원 2016. 8. 17. 선고 2014다235080 사건의 판단 이유를 일부 입법화한 것으로 해석된다.

대법원은 위 사건에서 "공개된 개인정보의 성격, 공개의 형태와 대상 범위, 그로부터 추단되는 정보주체의 공개 의도 내지 목적뿐만 아니라, 정보처리자의 정보제공 등 처리의 형태와 정보제공으로 공개의 대상 범위가 원래의 것과 달라졌는지, 정보제공이 정보주체의 원래의 공개 목적과 상당한 관련성이 있는지 등을 검토하여 객관적으로 판단"해야 한다는 기준을 제시한 바 있다. 하지만 이는 원칙적으로 대규모 프로파일링을 전제로 이루어진 판단이 아니므로, 대규모 프로파일링을 통한 개인신용정보의 활용을 전제로 한 신용정보법에는 적합한 기준이 아니다.

그런데 2020년 8월 4일 개정된 신용정보법 시행령은 이에서 더 나아가 제13조 제6호에서 상업적 목적과 비교형량하여 활용가능한 전제를 열어주고 있는바, 이런 취지로 사회·경제적 필요성과 개인정보 하나의 가치를 비교하는 것은 오히려 개인정보주체의 이익이 상업적 목적의 이익보다 낮게 평가될 우려가 크다. 따라서 신용정보법 시행령 제13조 제6호는 위 대법원 판결의 취지도 몰각한다는 점에서 개인정보의 권리침해의 우려가 크다.

(4) 신용정보법 시행령 제14조의2

신용정보법 시행령 제14조의2는 개인정보보호법 시행령상 정보집합물의 결합과 그 요건에 있어서 ①목적, ②절차, ③안전조치의 수준에 있어서 상이한데, 이러한 절차의 차이는 법정합성을 침해하고, 상업적 이용만을 강조하고 있다. ① 원칙적으로 결합의 기준과 내

용의 고시는 개인정보보호위원회가 정하도록 하고, ② 익명처리우선의 원칙을 결합에 있어서 도입하며, ③ 이종간 데이터의 결합에 있어서는 결합절차의 법정합성을 위하여 개인정보보호법이 정한 절차에 따르도록 정함이 필요하다.

(5) 신용정보법 시행령 제17조의2 제3항

신용정보법 제20조의2 제2항 제2호의2는 "가명정보를 이용하는 경우로서 그 이용 목적, 가명처리의 기술적 특성, 정보의 속성 등을 고려하여 대통령령으로 정하는 기간 동안 보존하는 경우"라고 규정하고 있다. 이에 따라 2020년 8월 4일 개정된 신용정보법 시행령 제17조의2 제3항은 "가명처리한 자가 가명처리시 정한 기간"이라고 정하고 있다.
그러나 위 신용정보법 조항은 신용정보제공자의 재량을 임의대로 허용한 것이 아니라 "그 이용목적, 가명처리의 기술적 특성, 정보의 속성 등을 고려하여 정"하도록 하고 있다. 따라서 신용정보의 특수한 사정이 고려될 이유가 없다면 개인정보보호법과 달리 해석될 이유가 없는 조항이다.

(6) 신용정보법 시행령 제21조의2 제1항 제1호

신용정보법 제25조의2 제3호는 "신용정보의 가공분석 및 제공 등과 관련하여 대통령령으로 정하는 업무"를 종합신용정보집중기관의 업무로 정하고, 시행령 제21조의2 제1항 제1호는 "신용정보를 활용하여 통계작성, 연구, 공익적 기록 보존 등의 목적을 위하여 가명처리 또는 익명처리한 정보로 제공하는 업무"라고 규정하고 있다. 그러나 해당 조항은 익명우선의 원칙이 포함되어야 하는바, 이러한 맥락에서 개인정보보호법과 법체계 정합성에 모순된다.

4. 상행위 거래정보의 시행령 입법의 문제점

금융위원회는 2020년 8월 4일 신용정보법 시행령을 개정한 직후 또 다시 동 시행령 제

28조의3 제6항 제5호에서 “신용정보주체의 거래내역을 확인할 수 있는 정보”를 규정함으로써 이러한 상행위 거래정보가 포괄적으로 개인신용정보의 전송요구대상으로 포함되었다. 이러한 내용은 앞서 본 2020. 8. 4. 개정 신용정보법 시행령 입법예고 당시에는 전혀 포함되지 않은 내용이었다.

금융위원회는 위 시행령의 근거조항으로 신용정보법은 상거래정보를 신용정보의 일종으로 입법화해 온 것을 근거로 주장하고 있다(개정전 신용정보법 제2조 나호, 개정전 신용정보법 시행령 제2조 제1항 제2호, 개정 신용정보법 제2조 제1호의3 마목).

한편, 금융위원회는 과거에는 비록 법적으로 해석가능하다 하더라도 개인정보보호법 또는 정보통신망법과의 관계 속에서 자제하여 개인신용정보로 포함시키지 않았다. 하지만 이제는 일반 시민들이 예측할 수 없는 범위의 정보까지도 모두 신용정보법의 적용대상에 포함시키려다 보니 이러한 문제가 불거지고 있다. 한 번 개인신용정보로 해석되어 수집된 정보는, 이후 신용정보법의 적용으로 개인정보보호법의 적용을 우회하여 개인정보주체의 통제권을 벗어나 활용의 대상이 될 것을 쉽게 예측할 수 있다. 특히 앞에서 본 바와 같이 신용정보법 시행령의 많은 부분들이 다시 포괄위임입법을 통해 고시로 재위임되고 있어 법령의 정확한 내용을 파악하기 힘들고 금융위원회의 유권해석으로 개인정보의 목적 외 활용을 지나치게 확대하고 있다는 점에서도 그러하다.

더 나아가 해당 조항이 참고한 유럽연합의 개인정보보호법상 개인정보 이동권은 정보주체의 통제권의 보장과 독점산업에 대한 대항장치로서 역할을 하려는 취지였다. 그러나 적극적으로 정보주체의 통제권을 형해화시키고, 개인정보보호법을 우회하는 신용정보법에서 이를 도입함은 정보이동권의 본질에 반하여 정보주체의 통제권을 형해화하는 제도로서 활용될 수밖에 없다.

5. 질병정보와 개인신용정보

금융위원회는 2020년 8월경 보험회사가 보유한 고객의 질병정보 등(개인의 질병, 상해 그 밖에 이와 유사한 정보, 이하 질병정보 등)을 가명처리한 가명정보는 정보주체의 동의 없이 제3자 제공, 활용 등이 가능하다는 유권해석을 내렸다. 금융위원회는 이에 따라 질

병정보 등을 신용정보법 제32조 제6항 제9호의2에 따라 “통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우”에는 정보제공자와 정보수령자가 정보주체의 사전동의를 받지 않고 타인에게 제공해도 된다고 유권해석하였다.
그러나 금융위원회의 이 같은 유권해석은 ① 개인의 질병정보 등은 개인신용정보가 아니라는 점, ② 그러한 측면에서 신용정보법 제33조 제2항에서 “질병정보 등”에 대해서는 사전에 동의를 받아 대통령령으로 정해진 목적으로만 수집, 조사 또는 제3자 제공할 수 있다고 규정하고 있는 점 등을 종합하여 해석하면 신용정보법에 반한 위법적인 해석이다.

질병정보 등은 그간 금융위원회에 의하여 개인신용정보에 해당하지 않는다고 유권해석되어 왔다. 특히 개정 전 신용정보법에서는 제23조 제1항 제2호에서 “개인의 질병에 관한 정보”를 개인신용정보로 포함하였다가, 반성적 고려하에 개인신용정보의 개념에서 개인의 질병정보가 삭제되고 오히려 질병정보 등에 대한 사전동의가 강화되고, 처리 목적이 대통령령으로 제한되는 개정이 이루어졌다(개정 전 신용정보법 제16조, 시행 2009. 10. 2., 법률 제9617호). 위 해당 조항은 개정 후 신용정보법 제33조로 조문 배열만 변경하여 여전히 유지되고 있다. 따라서 “질병정보 등”을 개인신용정보에 해당한다고 해석하거나, 개인신용정보에 적용되는 신용정보법상의 가명처리 조항이 “질병정보 등”에도 적용가능하다고 해석함은 신용정보법 명문의 규정에 반하는 위법한 주장이다.

더 나아가 앞서 상술한 것과 같이 신용정보법 제33조 제2항은 질병정보 등을 수집할 때 개인의 동의를 받고 시행령에서 정하는 목적으로만 이용하도록 하고 있다. 가령 금융위원회의 주장처럼 질병정보 등이 개인신용정보라 보더라도 이는 다른 조항에 우선해서 해석되어야 하는 특별규정인 신용정보법 제33조 제2항 위반이다. 민감정보의 사전동의를 요구하는 신용정보법 제33조 제2항과 목적외 제3자 제공의 예외를 인정하는 같은 법 제32조 제6항 제9호의2와의 관계는 개인정보보호법 제24조(민감정보)와 제18조 제2항 각 호(목적외 제3자 제공의 예외)와 그 체계가 동일한데, 그간 행정안전부는 개인정보보호법에 대해서는 제24조가 제15조, 제17조, 제18조에 우선하여 적용한다는 유권해석을 반복적으로 내려왔으므로 금융위원회도 동일한 취지의 해석을 내림이 마땅하다.

6. 결어

신용정보법과 동법 시행령이 개인정보보호법을 우회하려는 목적으로 도입되었다는 점에서 최초 법 개정시의 중요 취지였던 거버넌스 및 법체계 개선에 반하는 방향이다. 특히 이후 주문내역정보, 질병정보 등에 얽힌 문제들은 이러한 개인정보보호법 우회의 사례들로 앞으로도 유사한 일들이 계속적으로 발생할 수 있다. 이 사건 이후 주문내역정보, 질병정보와 관련하여 금융위원회가 개인정보보호위원회의 의견조회를 받았는지 문의하자 그러한 절차가 전혀 존재하지 않았다고 답변하였다.

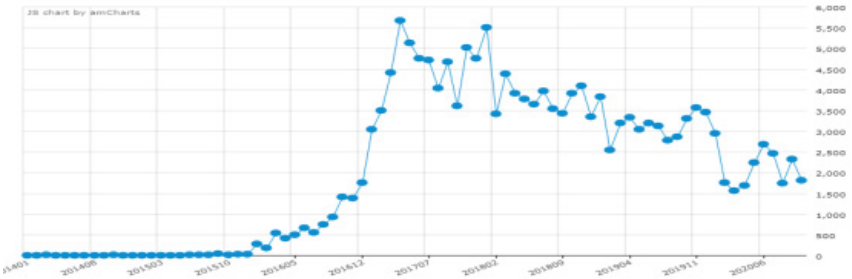
지금이라도 신용정보법은 개인정보보호법과 유사중복되는 조항을 모두 삭제하여 그 관할을 개인정보보호위원회로 이관하여야 하는 것이 시급한 일이고, 출범 초기 개인정보보호위원회가 집중적으로 거버넌스를 정비하여야 할 일이기도 하다.

02 개인정보 가명처리에 관한 동의

양홍석 변호사 (법무법인 이공)

1. '4차산업혁명위원회'의 출범과 규제철폐 논의

2016년 12월. '4차 산업혁명'이 회자되기 시작했다. 고도성장을 했던 한국경제는 1997년 IMF 외환위기를 거치면서 급전직하했고 어느 정도 회복세를 보였지만, 경제규모가 커지면서 과거와 같은 성장그래프를 그리지 못하는 상황이었다. 잠재성장률 전망은 우울했고, 당장 일할 곳을 찾지 못하는 이들이 넘쳐나고 살림살이는 점점 팍팍해졌다. 중국, 베트남 등 아시아 신흥국의 고성장은 이대로 뒤쳐질지 모른다는 불안으로 이어졌다. 이때 혜성처럼 등장한 개념이 '4차 산업혁명'이었다. 인공지능, 사물인터넷(IoT), 빅데이터, 로봇 등 신산업은 구체적이지는 않지만 SF 영화처럼 비현실적이지도 않았다. 암울한 현실과 대비되면서 더 도드라져 보였던 산업적 도약에 대한 동경과 기대가 '4차 산업혁명'을 신드롬으로 만들었다. 그 내용을 들여다보면 박근혜 정부의 '창조경제'와 닮아 있지만, 2016년말 박근혜 정부의 몰락과 함께 폐기된 '창조경제'를 대체할 만한 그 무엇이 필요했던 문재인 정부는 '4차 산업혁명'을 매력적인 어젠다로 활용했다. 그래서 2017~2018년에는 '4차 산업혁명'의 시대가 어느새 다가온 것 같은 느낌이 들기도 했다.

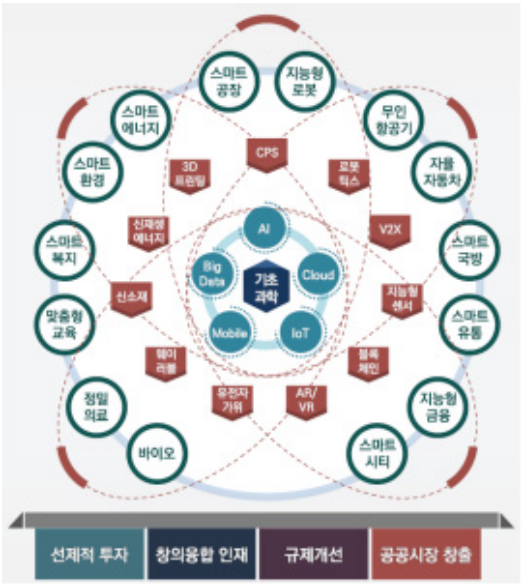


[그림-1] 빅카인즈 월간 키워드 '4차 산업혁명' 트렌드 분석결과(2014. 1. 1. ~ 2020. 10. 25.)

[그림-2] 2017. 10. 11. 4차산업혁명위원회 출범 및 제1차 회의

2017년 9월, '4차 산업혁명'을 위한 대통령 직속기구가 출범했고, 2017년 10월 11일 첫 회의에는 문재인 대통령도 참석해 힘을 실어줬다. 대통령이 참석한 회의에서 '4차 산업혁명'이 만들어낼 미래는 장밋빛 전망으로 채워졌다. 당시 문재인정부의 당면과제였던 "일자리창출"은 물론이고, 고착화된 저성장을 해결할 수 있는 대안으로 '4차 산업혁명'은 매력적인 소재였다. 그래서 문재인 정부는 '4차 산업혁명'을 시대적 과제로 끌어안았다. 2016년 이전에는 우리 사회 발전을 위한 방향이나 정책은 존재하지 않았던 것인 양 오래

된 구조적 문제들이 '4차 산업혁명'으로 일거에 해결될 것이라 믿었다.



[그림-3] 4차 산업혁명 관련 과학·기술-산업 간 연계도(출처: 4차산업혁명위원회 회의자료)

그런데 '4차산업혁명위원회(이하, '혁명위원회')'는 '규제·제도혁신 해커톤'으로 그 첫발을 내딛었다. 그 내용은 기존 규제의 철폐를 위해 1박 2일 12시간 동안 민관이 토론해서 결론을 도출하는 해커톤(Hackathon)을 한 것이다. 1박 2일 동안 토론한다고 해서 단번에 규제철폐·제도혁신을 위한 결론을 도출할 수 있다는 발상 자체가 문제를 지나치게 가볍게 보는 것이었지만, 더 큰 문제는 규제가 신산업을 막는다는 관념이었다. 규제가 산업발전을 막는다는 규제망국론으로 '4차 산업혁명'의 시대를 열어보겠다는 것이었다. 불필요한 규제를 없애는 것도 필요하겠지만, 규제가 없다고 해서 신산업이 융성할 것이라는 것은 막연한 기대에 불과하다. 혁명위원회의 첫 회의에서 제시한 자료에서도 선제적 투자, 창의융합 인재, 규제개선, 공공시장 창출 등 기반 위에 스마트 공장·에너지·환경·복

지·시티·유통·국방, 자율자동차, 무인항공기, 지능형로봇, 정밀의료, 바이오 등 분야별 산업이 발전할 수 있음을 제시했다. 그러나 규제 때문에 자율주행자동차, 지능형로봇, 스마트공장 등 산업이 융성하지 못한 것이 아니라 기술의 한계를 극복하는 것이 우선이다.

그럼에도 '혁명위원회'는 규제철폐를 기치로 내걸었고 대표적인 대상이 개인정보보호체계를 바꾸는 것이었다. 규제철폐는 정해진 결론이었고 개인정보보호를 위한 고민과 제안은 '혁명'의 시대에는 걸맞지 않은 것으로 무시했다.

2. 정보주체의 통제권을 약화시킨 '데이터3법' 개정

「개인정보 보호법」(이하 '개인정보보호법'), 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'), 「신용정보의 이용 및 보호에 관한 법률」(이하 '신용정보법') 등 3가지 법률 개정안들이 2020년 1월 국회에서 통과됐다. 4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 국가적 과제로 대두되었으니 "신산업 육성을 위해서는 인공지능(AI), 인터넷 기반 정보통신 자원통합(클라우드), 사물인터넷(IoT) 등 신기술을 활용한 데이터 이용이 필요하다"는데, 어떤 이론(異論)을 제기하기도 어려웠다. 그래서 결국 가명처리와 가명정보 개념의 도입, 가명정보 처리시 특례를 마련하고 가명정보의 결합도 가능하도록 하는 '데이터3법'이 탄생했다.

현행법상 '개인정보'는 살아있는 개인에 관한 정보로서 ①성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보, ②해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보, ③가명정보로 나눌 수 있다(개인정보보호법 제2조 제1호). '가명정보'는 위 ①, ②에 해당하는 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보를 말하고, 여기서 '가명처리'란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

그리고 가명정보의 가장 큰 특징은 통계작성, 과학적 연구, 공익적 기록 보존 등을 위하여 정보주체의 동의 없이 처리할 수 있고(개인정보보호법 제28조의2 제1항), 개인정보에 관한 정보주체의 권리가 대부분 박탈된다(개인정보보호법 제28조의7). 가명정보는 처리목적, 보유기간 제한이 없고, 유출된 경우에도 정보주체에게 통지할 필요가 없다. 정보주체가 열람·정정·삭제·처리정지를 요구할 수도 없고 수집·이용·제공에 관한 동의를 철회할 수도 없다. 신용정보법상 가명정보의 처리시에도 정보주체의 권리는 대부분 박탈된다(신용정보법 제36조 제6항, 제40조의3). 그래서 한국에서 '가명처리'는 정보주체의 권리를 박탈하는 과정이다.

3. 가명처리 vs 가명정보의 처리

개인정보보호법과 신용정보법상 '가명정보', '가명처리' 개념을 도입하면서 가명처리 후의 가명정보를 처리할 때 정보주체의 권리를 박탈하는 특례는 신설했으나, 개인정보를 가명정보로 만드는 '처리'에 관한 동의를 배제하는 규정은 만들지 않았다.

이로 인해 가명정보의 처리 특례를 둔 이상 정보주체의 동의 없이 가명처리도 가능하다는 입장[1]과 가명정보의 처리 특례를 뒀을 뿐 가명처리에 관한 특례를 두지 않았기 때문에 여전히 정보주체의 동의 없이 가명처리는 불가능하다는 입장[2]이 있을 수 있다. 그러나 개념상, 법문상, 시기상, 체계상 가명정보의 처리에 가명처리도 포함된다는 해석론은 설

1) 개인정보보호위원회가 2020. 10. 6. 사전공개한 『개인정보 보호법 해설서(안)』 221면에서는 가명정보의 처리에 관한 특례 중 제28조의2(가명정보의 처리 등) 규정에 관한 설명부분에서 "여기에서 가명정보의 처리는 개인정보의 가명처리를 포함한다"고 밝히고 있다. 그런데 개인정보보호법 제28조의2 '가명정보의 처리'에 개인정보의 가명처리가 포함된다는 근거는 제시하지 않았다.

2) 2020. 10. 14. 『개인정보 보호법 해설서(안)』와 관련한 온라인 설명회에서 해설서 발간에 관여한 김진환 변호사(김앤장 법률사무소)는 "향후 내 정보는 가명처리하지 말라고 요구할 수 있는 권리는 인정할 수 있는 것 아니냐는 이런 다양한 논의들이 있을 수 있거든요. 그런 부분들은 정책적으로 조금 더 논의를 해봐야 할 사안이 아닌가 생각됩니다."라고 설명했다. 토론자로 참석한 오병일 대표(진보네트워크)는 "가명정보와 가명처리는 다른 개념이거든요. 가명정보는 개인정보를 가명처리한 결과물이기 때문에 개인정보를 가명처리하는 데 대해서는 열람요구권, 처리정지권, 내 정보를 그렇게 처리하지 말라는 요구도 할 수 있어야 됩니다."라고 의견을 밝혔다.

득력이 없다. 먼저 개인정보보호법상 가명처리와 가명정보의 처리에 관하여 보면 아래와 같다.

첫째, 개념상 '가명처리'는 개인정보 '처리'의 결합이거나 '처리' 그 자체이다. 개인정보의 '처리'는 "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"를 의미한다(개인정보보호법 제2조 제2호, 신용정보법 제2조 제13호). '가명처리'는 "개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것"이다(개인정보보호법 제1조의2). 가명처리는 개인정보처리자가 보유한 개인정보 전부 또는 일부에 대해서 할 수 있다. 그래서 가명처리하는 목적에 따라 개인정보 중에서 가명처리할 대상정보를 추출하는 과정이 필요하다. 이 추출과정은 개인정보를 '검색'하고, '가공·편집'하거나 '연계·연동'하는 과정을 거쳐 이를 '편집·출력·이용'해 대상항목을 '저장'하는 것으로 이어진다. 그래서 '가명처리'는 개인정보처리자가 보유한 정보의 전부 또는 일부를 가명정보로 만들기 위해 개인정보의 다양한 '처리' 과정을 통칭하는 것으로 이해할 수 있다. 즉, '가명처리'는 개인정보의 다양한 '처리'가 결합된 것이거나 전제된 개념이다.

둘째, 가명처리는 가명정보의 처리와 시기상 구분된다. 개인정보의 전부 또는 일부를 추가정보 없이 특정개인을 알아볼 수 없는 형태로 처리하는 것이 '가명처리'이고, 가명정보는 가명처리의 결과다. 그래서 가명정보의 처리는 논리적으로 가명처리 이후에 비로소 존재할 수 있다.

셋째, 법문상 가명처리와 가명정보의 처리는 구분된다. 개인정보보호법상 '가명처리'는 정의규정에서 등장할 뿐 다른 규정에서 그 흔적조차 찾기 어렵다. 신설된 개인정보보호법 제3조 제6항에서 "개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한

다.”라고 규정하고 있다. 그러나 여기서 ‘가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우’에서 “가명으로 처리”라는 문구가 등장하지만, 이것은 가명처리 자체를 말하는 것이 아니라 가명정보의 처리를 의미하는 것이다. 왜냐면 가명처리 자체는 개인정보를 가명정보로 만드는 과정을 말하는 것인데, 그 가명처리로는 수집목적을 달성할 수 없고 가명처리한 정보(가명정보)로 처리함으로써 비로소 목적달성 여부를 판단할 수 있으므로 이 규정에서 “가명으로 처리”는 ‘가명정보로 처리’를 의미하는 것으로 보아야 한다.

한편, 개인정보보호법 제3장(개인정보의 처리)은 제1절 ‘개인정보의 수집, 이용, 제공 등’, 제2절 ‘개인정보의 처리제한’, 제3절 ‘가명정보의 처리에 관한 특례’로 나뉘는데, 제3절에서 “가명정보의 처리”를 명시하고 있다. 개인정보보호법 제28조의2 제1항, 제28조의5, 제28조의6에서 ‘가명처리’와 구분되는 개념으로서 “가명정보의 처리”에 관한 특례규정[3]을 신설했다. 이런 명문규정을 뛰어넘어 가명정보의 처리와 구분되는 가명처리도 특례규정의 적용을 받는다고 주장하는 것은 적절치 않다.

넷째, 가명처리와 가명정보의 처리는 개인정보보호법의 체계상 명확하게 구분된다. 가명처리는 그 대상정보가 그 자체로 개인을 알아볼 수 있거나 다른 정보와 쉽게 결합해 특정 개인을 알아볼 수 있는 정보를 대상으로 하고, 가명정보는 추가정보 없이는 개인을 알아볼 수 없다. 가명처리의 대상이 되는 정보와 가명정보는 개인식별성 여부가 다르기 때문에 보호의 방식과 수준이 다르다. 또 개인정보보호법 제3장 제3절 ‘가명정보처리에 관한 특례’에서는 가명정보의 결합, 안전조치, 처리시 금지사항 등에 관하여 별도로 규정하고 있을 뿐 가명처리시 준수해야 할 기준에 관하여는 전혀 정하지 않고 있다. 개인정보보호법 제28조의7(적용범위) 규정 역시 ‘가명정보’에 대해서는 정보주체의 권리를 배제하도

3) 개인정보보호법 가명정보의 제3자 제공(제28조의2 제2항), 가명정보의 결합(제28조의3)을 ‘가명정보의 처리’와 병렬적으로 규정하고 있는 것으로 보이지만, 이 제3자 제공, 결합 모두 제3절 ‘가명정보의 처리에 관한 특례’에 속하는 것이고 제71조(벌칙) 제4의2호에서 제28조의3(가명정보의 결합)을 위반해 가명정보를 ‘처리’하는 경우를 처벌하고 있어 가명정보의 결합은 가명정보 처리의 한 유형으로 볼 수 있다.

록 정하고 있을 뿐 '가명처리'에 관해서는 아무런 규정을 두지 않고 있다.[4)]

신용정보법도 개인정보보호법의 규정체계와 기본적으로 동일해서, 신용정보법상 가명처리와 가명정보의 처리는 명확하게 구분된다. 신용정보법상 '처리'(제2조 제13호)는 개인정보보호법상 '처리'의 개념과 동일하고, 가명처리(제2조 제15호)와 가명처리한 개인신용정보인 가명정보(제2조 제16호) 역시 개인정보보호법상 가명처리, 가명정보와 본질적으로 같다. 가명정보의 이용과 가명처리를 명시적으로 구분하고(제20조의2 제2항 제2호의2, 제32조 제6항 제9호의2 또는 제9호의4, 제40조의2), 가명정보나 가명정보를 이용하는 경우에 관하여만 적용제외 규정을 두고 있다(제32조 제6항, 제40조의3).

이와 같이 가명처리와 가명정보의 처리는 '데이터3법' 처리 이후의 개인정보보호법, 신용정보법상 명확하게 구분되는데, 해석을 통해 가명처리를 가명정보의 처리에 포함된다거나 개인정보 처리에 관한 일반원칙을 배제하는 것은 '법창조'로 허용될 수 없다. 그래서 개인정보를 가명정보로 만드는 '가명처리'에는 개인정보 처리에 관한 일반원칙이 그대로 적용된다. 즉, 가명처리도 개인정보 처리에 해당하므로 수집시 이용목적으로 '가명처리'가 명시되어야 하고, 가명처리에 대해 동의했더라도 철회할 수 있다.

4. 가명처리에 대한 동의와 동의의 철회

'데이터3법'은 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 경우에는 정보주체의 동의를 받지 않아도 된다. 가명정보의 특성상 정보주체를 특정(재식별)하기 어렵기 때문에 특정 정보주체의 권리를 보장하기 어렵다는 전제에서 정보

4) 20대 국회에서 인재근 의원이 2018. 11. 15. 대표발의한 개인정보보호법 개정안(의안번호 2016621) 제28조의7은 가명정보로 만드는 '가명처리' 와 가명정보화된 이후인 '가명정보의 처리'를 명확하게 구분했고, '가명처리'도 정보주체의 동의없이 할 수 있도록 하는 특례를 뒀었다. 그런데 이 '가명처리'에 관한 특례규정은 2019. 11. 27. 개인정보보호법 대안이 만들어질 때 제외되면서 '가명처리'는 여전히 정보주체의 동의가 필요한 상태로 남게된 것이니 이런 입법연혁을 고려해도 '가명처리'와 '가명정보의 처리'는 명확하게 구분해야 한다.

주체의 권리를 보장하지 않는 특례를 도입한 것이다. 대신 가명정보의 처리시 일정한 제한을 둠으로써 무분별한 가명정보의 활용을 막고자 한 것이다.

국회 입법과정을 보더라도, 가명처리한 후에 가명정보를 어떻게 활용할 것인지, 민감정보의 가명처리 후 활용이 가능할 것인지에 관하여만 논의가 있었을 뿐 가명처리 자체를 정보주체의 동의 없이 할 수 있다고 보지 않았다. 아마도 이렇게 논의가 전개된 것은 '데이터3법' 개정 과정에서 참고한 EU GDPR의 영향 때문으로 보인다. GDPR에서 가명처리(pseudonymisation)는 개인정보를 처리할 때 위험성을 감소시키는 보호조치로서, 개인정보 처리의 당초 목적과 양립가능성 여부를 판단할 때 고려요소로 활용하고(GDPR 전문 제50항 및 제156항, 제6조 제4항[5]), 공익을 위한 기록 보존 목적, 과학적·역사적 연구 목적 또는 통계 목적을 위한 개인정보의 추가 처리는 가명처리 등 안전한 조치를 취하는 한 원래 목적과 양립 가능한 것으로 보기 때문에(GDPR 본문 제5조 제1항 (b)) 특정한 목

5) KISA GDPR대응센터 페이지(https://gdpr.kisa.or.kr/gdpr/static/gdprProvision.do) 중 GDPR 조문비교 참조.

GDPR 원문

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship etween data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

GDPR 번역문

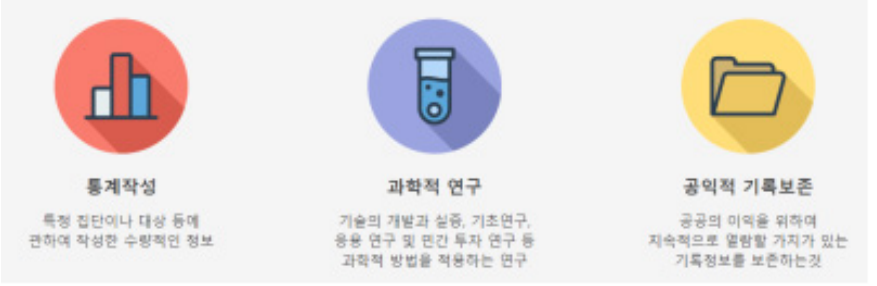
4. 개인정보를 수집한 목적 외로 처리하는 것이 개인정보주체의 동의 또는 제23조(1)의 목적을 보장하기 위한 민주사회의 필요하고 비례적인 조치를 구성하는 유럽연합 또는 회원국 법률에 근거하지 않는 경우, 컨트롤러는 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 특히 다음 각 호를 고려해야 한다.
(a) 수집 목적과 의도된 추가처리 목적 간의 연관성
(b) 특히 개인정보주체와 컨트롤러 간의 관계와 관련해서 등의 개인정보가 수집된 상황
(c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격
(d) 의도된 추가처리가 개인정보주체에 초래할 수 있는 결과
(e) 암호처리나 가명처리 등 적절한 안전조치의 존재

적을 위한 가명처리시에는 정보주체의 동의가 필요없다는 전제가 형성된 것이다. 그런데 GDPR의 경우, 공익적 목적이 있는 경우 정보최소화원칙(the principle of data minimisation)을 준수하기 위한 적정한 안전조치로서 가명처리를 제시한 것이고, 이 경우 정보주체의 열람권, 정정권, 처리제한권, 처리거부권, 반대권 등의 일부 권리의 적용을 제외할 수 있다는 것이다(GDPR 제89조).

반면, 우리 '데이터3법'은 위에서 본 것과 같이 가명정보 처리의 목적과 관련없이 일반적으로 정보주체의 권리를 박탈하는 형식을 취하고 있고(개인정보보호법 제28조의7, 신용정보법 제40조의3), 특정한 목적을 위한 가명정보의 처리시 정보주체의 동의를 받지 않아도 되도록 규정하고 있다(개인정보보호법 제28조의2, 신용정보법 제32조 제6항 제9호의2). 또 GDPR은 개인정보를 수집할 때 처음부터 개인정보의 처리 목적을 구체적이고 명시적으로 제시해야 하고, 적법한 목적을 위해서 수집해야 하며 최초 수집 목적과 부합하지 않는 방식의 추가 처리를 하지 않는다는 '목적 제한(purpose limitation)의 원칙'의 예외로서 공익적 목적이 있는 경우의 활용을 언급함으로써 개인정보의 추가적 이용 또는 제공과 공익적 목적이 있는 경우의 추가적 이용 사이의 '관련성'을 명확하게 제시했다. 그러나 우리의 경우 개인정보보호법상 '개인정보의 추가적인 이용 또는 제공'(제15조 제3항, 제17조 제4항)이나 신용정보법상 '당초 수집한 목적과 상충되지 아니하는 목적으로 제공하는 경우'(신용정보법 제36조 제6항 제9호의4)와 공익적 목적을 위한 가명정보의 처리를 분리함으로써 두 규정 사이의 관련성을 제거했다. 이로 인해 GDPR과는 법문의 체계와 형식이 달라지게 된 것이다. 그래서 GDPR에서의 당연한 전제가 우리 '데이터3법'의 법문과 체계상 당연히 통용될 수 없게 된 것이다.

5. 우리 법상 가명처리의 목적은 제한되는가

개인정보보호위원회가 2020년 9월에 공개한 『가명정보 처리 가이드라인』 12면에서는 가명처리의 사전준비과정에서 "가명정보의 처리목적 명확화 : 법률에서 허용하는 목적 내에서 가명정보를 처리하는 목적을 최대한 명확히 작성하여야 함. 통계작성, 과학적 연구, 공익적 기록보존 등에 한함"이라고 설명하고 있다.



[그림-4] 가명정보 처리 대상 (출처 : 개인정보보호위원회)

금융위원회가 2020년 8월 공개한 『금융분야 가명·익명처리 안내서』 17면에서도 『가명정보 처리 가이드라인』과 같이 "가명정보의 활용 목적은 「신용정보법」에서 허용하는 목적 내에서 최대한 구체화 ※ 통계작성(상업적 목적 포함), 연구(산업적 연구 포함), 공익적 기록보존 목적 등"이라고 설명하고 있다.

개인정보보호법, 신용정보법의 규정상 통계작성 등 특정한 목적이 있는 경우에는 정보주체의 동의 없이 가명정보를 처리할 수 있는 규정을 뒀을 뿐인데, 이 규정을 특정한 목적의 존재를 가명처리의 허용조건으로 해석하는 것이다. 이런 해석론은 GDPR 제89조 적용을 전제한 해석론을 그대로 가져온 것이다.

개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리해야 한다(개인정보보호법 제3조 제6항)는 원칙은 '데이터3법' 처리 이전부터 존재했다. 그런데 여기에 더해 '데이터3법' 처리시 '개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다'(개인정보보호법 제3조 제7항)는 규정을 신설했다. 가능하면 익명처리하고, 익명처리로 안 될 경우에는 가명처리하라는 것이다. 그리고 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의없이 가명정보를 처리할 수 있다(개인정보보호법 제28조의2 제1항).

여기서 개인정보보호법상 가명처리는 권장되는 것이니 특정한 목적(통계작성, 과학적 연구, 공익적 기록보존)이 없이 수집목적 달성에 적합해서 가명처리하는 경우도 있을 수 있지 않냐는 의견도 있을 수 있다. 개인정보보호법 제28조의2 제1항에 따라 특정한 목적을 위하여 가명정보를 처리하는 경우에는 정보주체의 동의를 받지 않아도 된다. 이 규정의 반대해석상 이런 특정한 목적이 있는 경우에는 정보주체의 동의 없이 가명정보를 처리할 수 있다는 것이므로, 이런 특정한 목적이 없더라도 정보주체의 동의가 있다면 가명정보의 처리가 가능하다. 그 외에 가명정보에 대한 정보주체의 권리를 박탈하는 규정(제28조의7) 역시 법문의 형식상 "가명정보"에 관한 것일 뿐 목적을 따로 요구하지 않는다.
신용정보법상 개인신용정보의 제공·활용에는 원칙적으로 신용정보주체의 동의가 필요한데, 통계작성(상업적 목적 포함), 연구(산업적 연구 포함), 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우에는 예외적으로 동의를 받지 않아도 된다(신용정보법 제32조 제6항 제9호의2). 이 규정은 개인정보보호법 제28조의2 제1항과 구조가 동일하다. 다만, 신용정보법에는 개인정보보호법 제3조 제7항과 같이 가능하면 익명정보로 처리하고, 익명정보로 안 될 경우에는 가명정보로 처리하라는 규정이 없다. 그러나 개인정보보호법 제3조 제7항과 같은 규정이 없다고 해도 신용정보법 제32조 제6항 제9호의2가 가명처리의 목적을 제한하는 규정으로 볼 수 있을지 의문이다. 결국 신용정보법상 가명정보 제공의 목적에 따라 예외적으로 신용정보주체의 동의 없이 처리할 수 있도록 규정한 것일 뿐 신용정보주체의 동의가 있는 경우에는 통계작성 등 특정한 목적이 없는 경우에도 가명처리가 가능하다.

그런데 GDPR의 해석론을 차용하고 GDPR 제89조를 중심으로 한 규정에 집중한 탓에 GDPR에서 '가명처리'가 어떤 지위를 갖는지 간과했다. GDPR은 '가명처리'를 정보주체의 권리를 박탈·제한하는 절차로 삼는 것이 아니라 일반적인 위험감소절차로 규정하고

있다(GDPR 제32조 제1항 (a),[6] 제40조 제2항 (d)). GDPR에서의 '가명처리'는 일반적 보호조치로서 규정된 것이다.

결국 개인정보보호위원회, 금융위원회의 '해설'은 GDPR 제89조 외의 다른 규정과도 충돌하는 것이고 우리 법의 규정형식·내용과도 어긋나는 것이다. 우리 법에서는 가명정보에 관하여 정보주체의 권리를 제한함으로써 가명처리를 정보주체의 권리를 박탈하는 절차로 만들어 버렸고, 개인정보의 추가적 이용·제공과 공익적 목적을 위한 가명정보의 처리를 분리해 양자의 '관련성'을 제거하면서 우리는 우리 법의 내용과 형식에 맞는 해석을 할 수밖에 없게 됐다. 그래서 가명처리에 대한 정보주체의 '동의'는 여전히 유효하고, '동의'한 후의 동의철회도 가능하다고 봐야 한다.

6. 가명정보의 처리는 정보주체가 상상할 수 없는 위험

이제까지는 공공기관이든, 기업이든, 개인이든 개인정보처리자들은 각자 개인정보를 처리했다. 정보주체가 A회사의 서비스를 이용할 때, 원칙적으로 그 정보가 B회사에 제공되지 않는 환경에서 개인정보의 수집·이용에 관한 동의를 해왔다. 그리고 예외적으로 제3자에게 제공하는 경우에는 명시적인 동의를 받기 때문에 정보주체는 정보제공의 상대방을 선택하고, 그 상대방에게 제공하는 정보의 종류와 양을 결정함으로써 스스로 자기정

6) KISA GDPR대응센터 페이지(https://gdpr.kisa.or.kr/gdpr/static/gdprProvision.do) 중 GDPR 조문비교 참조.

GDPR 원문

Article 32 Security of processing
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate
(a) the pseudonymisation and encryption of personal data;

GDPR 번역문

제32조 처리의 보안
1. 컨트롤러와 프로세서는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 해당 위험에 적정한 보안 수준을 보장하기 위해 특히 다음 각 호 등을 포함하여 적정한 기술 및 관리적 조치를 이행해야 한다.
(a) 개인정보의 가명처리 및 암호처리

보를 '관리'할 수 있었다. 이렇게 정보제공의 상대방, 정보제공 여부를 결정함으로써 특정 개인정보처리자가 운용하는 서버로의 정보유입, 해당 서버로부터의 정보유출을 정보주체가 통제할 수 있는 절차가 존재했다.

그런데 가명정보의 처리로 이런 정보주체의 '관리'는 무의미해졌다. 특정 개인정보처리자가 운용하는 서버 내에서만 존재했던 개인정보가 가명처리된 후에는 가명정보 처리의 특례에 따라 제3자에게 제공된다. 여기서 정보주체는 철저히 소외되어 있다. 제3자에게 제공되는 지를 알 수 없고, 알더라도 막을 수 없고 처리를 정지하도록 할 수도 없다. 여기에 가명정보의 결합까지 허용되면서 정보주체가 자신의 개인정보를 분산·관리하더라도, 개인정보처리자의 필요와 선택에 따라 정보주체가 분산해 둔 정보가 결합되고 이렇게 결합된 데이터가 결합신청을 한 개인정보처리자에게 다시 반출되는 길까지 열려있다. 가명처리된 이후 정보주체의 권리가 단절되면서 상상할 수 없었던 위험에 직면하게 된 것이다.

7. 가명정보의 결합을 위한 가명처리 동의

2020년 8월 6일 신한카드와 SK텔레콤은 이종데이터를 결합한 '가명정보 결합상품'을 출시하겠다고 발표했다. 양사가 각자 보유한 고객데이터를 가명처리한 가명정보를 결합하겠다고 밝혔다.

신한카드는 2020년 8월 5일 『개인정보 처리방침』을 개정하면서 제1조(개인정보의 처리목적)에 "11. 통계작성(상업적 목적포함), 연구(산업적 연구 포함), 공익적 기록보존 목적 등으로 가명처리에 이용"을 추가했다. SK텔레콤도 2020년 8월 5일 『개인정보 처리방침』을 개정하면서 "SK텔레콤은 수집한 개인정보를 특정 개인을 알아볼 수 없도록 가명 처리하여 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리할 수 있습니다."라는 규정을 추가하였고, 가명정보의 처리에 관한 규정 등을 신설했다. 신한카드와 SK텔레콤이 2020년 8월 6일 가명정보 결합을 발표하기 하루 전에 가명정보의 처리에 관한 규정뿐만 아니라 '가명처리'를 개인정보처리의 목적으로 추가한 것은 개인정보보호법과 신용정보법상 가명처리에 관한 정보주체의 동의가 여전히 필요하다는 판단에 따른 것이다. 앞

으로 가명정보를 활용하고자 하는 많은 기업, 공공기관 등이 이런 식으로 약관이나 개인정보 처리방침에 "통계작성(상업적 목적 포함), 연구(산업적 연구 포함), 공익적 기록보존 목적 등"으로 가명처리할 수 있음을 명시할 것으로 보인다.

8. 가명정보의 세계에는 정보주체의 자리가 없다

이런 방식이 적합한가? 가명처리는 가명처리의 결과물인 가명정보에 대한 정보주체의 통제권을 제거하는 과정이다. 정보주체로서는 자신의 개인정보가 가명정보의 세계로 넘어가지 않도록 진입통제를 하는 것 외에는 다른 통제수단이 없다. 그래서 이 가명처리에 대한 '동의'는 형식적으로는 처리에 대한 동의지만, 실질적으로 정보주체로서의 권리를 포기하는 것이다. 법문상 가명정보의 처리가 가능한 목적(통계작성, 연구, 공익적 기록보존)을 『개인정보 취급방침』에 나열하거나 약관에 넣고, 이에 동의했다고 해서 가명처리에 대해 동의한 것으로 본다면, 가명정보 활용에 저항할 수 있는 유일한 권리를 무력화하는 것이다. 최소한 언제, 어떤 목적으로, 어떤 항목들을, 어떤 수준으로 가명처리할 것인지 구체적으로 제시하고 가명처리 전에 사전동의를 받도록 해야 한다. 그런데 현실은 '필요에 따라 가명처리할 수 있다'라는 규정을 신설한 『개인정보 처리방침』 개정으로 포괄적 동의마저 흔들리고 있다.

9. 가명처리를 막을 수 있는 저항권

2020년. 일상은 디지털화된 정보 생성·소비를 빼고 말하기 어렵다. 디지털기기 사용이 늘어나면서 일상생활을 하면서 남긴 디지털 흔적들이 자동화된 시스템에 의해 매순간 디지털화된다. 개인의 일상 자체가 디지털 정보로 미러링(mirroring)되고 있다고 해도 과언이 아니다. 의식하지 못하는 가운데, 원하지 않아도, 일상이 매순간 디지털정보로 기록되고 있다. 이 정보들은 어딘가에 저장되고, 어딘가로 보내지고, 가공·사용된다. 이런 개인정보의 디지털화는 개인정보의 수집·보관·가공·활용·유통 등 모든 면에서 질적인 변화를 가져왔다. 여기에 더해 개인정보처리자들 사이에서 제한적으로 이루어지던 데이터 유

통을 가로막고 있었던 둑을 '데이터3법'이 없애버렸다. 개별 데이터 서버에 있던 정보들이 가명처리를 거쳐 가명정보의 바다로 흘러갈 것이다.

이 거대한 흐름을 되돌리기는 어려울 것이다. 과학기술은 발전하고, 데이터 활용이 당연시되는 '혁명의 시대'에 이미 진입했는지 모른다. 그런데 왜 개인정보의 수집·이용에 대한 '동의'를 구하는 방식은 큰 변화가 없을까? 왜 '동의'를 좀 더 효과적으로, 효율적으로 얻는 것은 기술적 진보의 대상에서 소외되었을까? 정보주체로부터 데이터를 어떻게 가져갈 것인지 보다 가져간 데이터를 어떻게 쓸 것인지에 더 집중하는 것은 이해할 수 있지만, 최소한 그 데이터가 사람에 관한 것이라는 점은 잊지 말아야 한다. 웹상에서 하루에도 몇 번씩 만나는 '동의', '동의'를 클릭하기 전에는 '다음'을 기대할 수 없는 설계에는 이미 익숙해졌지만, 실질적으로 결정할 수 있는 그 무엇은 남겨지길 바란다. 형식적 동의가 일상이 된 시대를 살아가는 사람들로부터 마지막 남은 형식적 동의 전까지 박탈하는 '가명정보'의 활용은 누구를 위한 것인가? 분명한 것은 정보주체는 그 이익을 누리지 않는다. 그래서 권리를 박탈하는 가명처리에 순응해야 하는 이 기이한 시스템은 폭력적이다. 인간에 대한 존중이 없는, 비즈니스로 전락한 데이터 활용에 저항할 수단이 필요하다. 나에 대한 정보를 실질적으로 통제할 수 없는 세계에서 개인은 그 존재 의의를 찾기 어렵다.

점점 개인이 사라져 가는 세상에서 프라이버시를 지키는 유일한 수단이 가명처리에 관한 동의권이다. 사전동의(OPT-IN)든, 동의철회(OPT-OUT)이든, 디지털화되는 정보를 지키는 저항권이 될 수 있다.

03 한국의 마이데이터 문제점과 소비자권리

정지연 사무총장 (한국소비자연맹)

1. 서론

코로나19로 촉발된 사회의 변화는 일상생활을 포함한 모든 생활에서 소비자에게 큰 변화를 요구하고 있다. 언택트 환경에서 사회가 빠르게 디지털화되면서 데이터 경제시대에 소비자의 역할이 강화되고 편익이 향상될 것이라는 긍정적인 기대와 함께 소비자 권리 침해로 인한 소비자 문제가 심화될 수 있다는 우려가 함께 제기되고 있다.
데이터 활용 및 데이터산업 활성화를 위해 여러 나라에서 법·제도를 정비하고 있는데, 유럽연합의 경우 2016년 기존의 「EU 개인정보보호지침」을 「일반개인정보보호규정」(General Data Protection Regulation: GDPR)으로 개정하면서 개인정보 이동권(Right to data portability)을 신설하였다.

개인정보 이동권은 정보주체가 본인 데이터에 대한 전송을 요청하면, 개인정보처리자는 보유한 데이터를 정보주체에게 또는 정보주체가 지정한 제3자에게 전송하는 정보주체의 권리이다.[1] 그런데 우리나라는 마이데이터의 근간이 되는 정보이동권이 일반적인 개인정

1) 박훤일, "정보이동권의 국내 도입 방안", 경희법학 제52권 제3호, 경희법학연구소, 2017, 211-232면.

보 처리 및 보호에 관한 법률인 「개인정보 보호법」(이하 '개인정보보호법')이 아닌 신용정보에만 적용되는 「신용정보의 이용 및 보호에 관한 법률」(이하 '신용정보법')에만 규정되어 있어 이에 대한 한계가 있어 한국의 마이데이터의 문제점과 소비자권리에 대해 살펴보고자 한다.

2. 마이데이터와 구매정보

최근 금융위원회가 마이데이터 사업에 제공해야 할 신용정보 범위에 소비자가 인터넷쇼핑을 하면서 물품을 구매한 정보인 '주문내역 정보 등과 전용카드 이용내역'(이하 '주문내역 정보 등') 등이 포함된다고 하면서 논란이 되고 있다.

마이데이터 사업은 소비자가 동의한다면 흩어져 있는 은행이나 카드, 보험, 결제, 증권정보 등을 모아 맞춤형 금융서비스를 받을 수 있는 사업으로 정보주체의 데이터 이동권을 기반으로 새로운 금융서비스 제공이 가능할 것이라고 주장하고 있다. 문제는 마이데이터 사업이 신용정보법에만 그 근거가 있고 주문내역 정보를 개인신용정보로 확대해석 해서는 안 된다는 점이다. 민감한 개인정보인 거래내역을 이렇게 확대적용 한다면, 소비자의 입장에서 개인정보보호법과 신용정보법 중 어떤 것을 적용해야 할지 혼란스러울 수 있고 이는 향후 개인정보보호 체계를 위협할 수 있다. 마이데이터 사업이 개인정보의 활용을 중심으로 상업화를 추진하고 있는 금융위원회 관할로 들어갈 때 개인정보가 제대로 보호될 수 있을 것이라고는 소비자의 입장에서 기대하기 어렵다.

전자상거래 시장이 확대되고 모바일 거래까지 활발해지면서 전자상거래를 통한 거래가 광범위해지고 있어 인터넷쇼핑몰 주문내역 정보 등을 통해 개인의 일거수 일투족이 노출될 가능성이 매우 높아지고 있다. 소비자는 호텔 등 숙박, 여행, 취미생활, 콘텐츠 구매 등 개인이 민감하게 생각하는 정보까지 마이데이터 사업에 제공할 수 있다고 생각하기 어렵고 모아진 데이터들이 가명화된 형태로 상업적으로 활용될 수 있다는 것을 충분히 알기 어렵다. 특히 우려되는 점은 시계열로 분석한 정보를 마이데이터 사업자가 수입해 저장

한다는 부분이며 소비자 입장에서 이 정보들이 어떻게 활용될지 예측하기 어렵다는 점이 더 큰 문제이다.

2020년 1월에 통과된 데이터3법(개인정보보호법, 정보통신망법, 신용정보법) 중에서 소비자·시민단체 안에서 특별히 신용정보법에 대한 우려가 매우 컸다. 신용정보법의 경우 동법 시행령의 많은 조항이 법에서 위임받은 주요 부분을 다시 고시로 재위임하고 있어 법령의 정확한 내용을 파악하기 힘든 문제점이 있고, 개인정보의 목적 외 활용을 지나치게 확대하려는 부분에 대한 우려가 있다. 특히 이번 주문내역 정보 등의 경우 2020년 3월 동법 시행령 입법예고안에는 관련 내용이 없었으며 8월 공표된 동법 시행령에 갑자기 등장하며 논란이 되었다. 하지만 금융위원회는 주문내역 정보 등을 신용정보라고 주장하며 문제가 없다는 입장이다. 신용정보법은 신용정보를 "상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보로서…"라고 규정하고 있으며, 더구나 문제가 되는 동법 시행령 제2조 제23항의 위임 법률인 신용정보법 제2조 제1호의3은 "신용정보주체의 거래내용을 판단할 수 있는 정보에 대하여 신용정보제공·이용자에게 신용위험이 따르는 거래로서 다음 각각의 거래의 종류, 기간, 금액, 금리, 한도 등에 관한 정보"로 특정하여 위임하고 있다는 점에서 주문내역 정보 등은 신용정보주체의 거래내용에 포함될 수 없음은 명확하다. 금융위원회가 위임입법의 한계를 넘어서까지 소비자가 '무엇을, 언제, 얼마에 샀는지'가 개인의 신용평가를 위해 왜 필요한지 또 소비자가 그 정보를 마이데이터 사업자에게 제공하도록 규정한 이유에 대해 명확하게 하는 것이 필요하다. 만약 확대 해석해 신용정보라고 한다면 마이데이터 사업자에게 제공되고 활용된다는 내용에 대해서는 정보주체인 소비자의 별도 동의절차가 필요할 것이다.

유럽연합의 GDPR 개인정보 이동권의 취지는 정보주체의 권리를 보호함과 동시에 데이터 독점을 막고 경쟁을 촉진하기 위한 것이다. GDPR 제20조의 '개인정보 이동권(Right

to data portability)'은 정보주체가 컨트롤러[2]에게 제공한 본인의 개인정보를 체계적으로 구성하여 기계판독이 가능한 형식으로 제공받을 권리를 의미한다. 정보주체는 기술적으로 실현 가능한 경우 개인정보가 한 정보 관리자에게서 다른 정보 관리자에게로 직접 전송되도록 할 권리가 있다. GDPR은 개인정보 이동권을 통해 정보주체에게 본인 데이터를 다른 정보처리자에게 이전할 수 있는 선택권을 제공하였다. 또한 구글, 페이스북, 애플, 아마존과 같은 미국 IT 플랫폼 기업들과 경쟁 관계에 있는 다른 정보처리자에게 소비자가 이전할 수 있게 하여 앞서의 거대 플랫폼 기업의 시장 지배력을 막고자 하였다.[3]

그러나 한국의 마이데이터 사업은 개인정보의 상품화를 촉진하는 것으로 변질되었다. 마이데이터 사업 활성화 이전에 소비자의 개인정보보호를 엄격하게 하기 위한 제도적인 보완이 우선되어야 할 것이다.

3. 향후 과제

우리나라의 경우 유럽연합과 같이 마이데이터 정책은 데이터 활용을 통한 편의성 증대뿐만 아니라 정보주체인 개인의 정보이동권 등 권리보장을 목표로 하고 있다. 그러나 앞서 언급한 바와 같이 한국의 마이데이터는 그 도입취지와는 다르게 개인정보의 상품화를 촉진하는 것으로 변질되었다.

현행과 같이 개인정보보호법이 아닌 금융 관련법인 신용정보법만으로 개인정보 이동권을 규율할 경우, 정보주체의 권리보다 금융서비스 산업의 데이터 유통 활성화 측면만이 강조될 우려가 있다.

이동권 행사를 위한 구체적인 동의 방법에 대한 논의가 이루어지지 않았으며, 개인정보

2) 컨트롤러는 개인정보의 처리 목적 및 수단을 단독 또는 제3자와 공동으로 결정하는 자연인, 법인, 공공기관, 에이전시, 기타 단체를 의미한다.

3) 송미정·김인석, "유럽 PSD2 시행에 따른 금융분야 마이데이터 정책의 개인정보보호 강화 방안 연구", 정보보호학회지 제29권 제5호, 한국정보보호법학회, 2019, 1205-1219면.

의 자기관리를 위한 개인정보자기관리툴(Tool)에 대한 개발도 미진한 상황이다.
개인정보자기결정권 및 이동권 행사 등의 방법에 대한 구체적인 관리체계의 개발 없이 마이데이터 사업이 시행될 경우, 개인은 서비스 이용을 위해 수동적으로 약관에 동의하고, 정보 이동 이후에는 자신의 정보가 어떻게 사용되고 있는지 알 수 없는 등 정보의 주체로서 역할을 할 수 없게 될 우려가 있다.[4)]
데이터 사용과 활용에 있어 소비자가 관련 내용을 정확하게 알고 판단할 수 있도록 구체적으로 동의절차를 마련하는 것이 필요하고, 원치 않을 경우 이를 철회하는 과정도 투명하고 명확하게 제시되어야 할 것이다.

마이데이터가 잘 정착하고 활성화되기 위해서는 정보주체인 소비자의 권리를 보장함으로써 신뢰가 기반이 되는 환경을 만들어야 하는데, 이를 위해 개인정보보호법에 개인정보 이동권을 신설해 소비자의 데이터 전반에 대한 보호가 이루어지는 것이 필요하다.
또한 2020년 8월 5일 통합 개인정보보호위원회가 출범했지만 금융위원회가 담당하는 금융분야는 개인정보보호위원회 권한이 미치지 못하는 것으로 해석되고 있어 이에 대한 개선도 함께 이루어져야 할 것이다. 개인정보의 보호와 활용 간의 조화와 균형이 어느 때보다 중요한데, 흩어져 있는 개인정보의 문제를 일관성 있고 종합적으로 판단할 수 있도록 금융 분야에 대한 감독기구도 개인정보보호위원회로 일원화하고 그 역할을 강화하는 것이 필요할 것으로 생각된다.

4) 조성은, “해외 개인정보 이동권과 마이데이터”, 국회입법조사처 전문가간담회, 2020. 9. 1.

04 개인정보보호 자율규제와 사회적 가치
EU GDPR의 함의

김태오 교수 (창원대학교)

1. 개인정보보호 자율규제와 사회적 가치의 관계

개인정보는 헌법상 보호의 대상이다. 개인정보는 헌법상 기본권인 개인정보자기결정권으로 보호된다. 「개인정보 보호법」(이하 '개인정보보호법')은 헌법상 보호대상인 개인정보의 보호를 법률 차원으로 구체화한 것이다.

개인정보보호법은 전형적인 규제의 영역이다. 개인정보보호법을 위반하면 행정제재와 형사처벌의 대상이 된다. 그러나 개인정보는 정부의 규제로 완벽히 보호될 수 없다. 오히려 100%의 개인정보보호는 불가능하다. 데이터가 주요 생산요소인 데이터경제 시대에서, 개인정보가 어떻게 수집·이용되는지를 정보주체가 파악하고, 이를 정부가 전부 감독하기란 불가능에 가깝다. 또한, 장래의 기술발전에 따른 개인정보 활용의 양상을 미리 예측하여 법요건으로 제도화할 수 없다.[1] 뿐만 아니라, 개인정보보호를 위해 필요한 규제이지만, 입법과정에서의 문제로 제도화에 어려움을 겪을 수도 있다. 이처럼 개인정보보호를 위한 규제는 불완전성이 전제될 수밖에 없다. 정부의 규제를 통한 개인정보보호의 수준에는 일정한 한계가 존재하는 것이다.

1) Sebastian Schulz, Privacy by Design - Datenschutz durch Technikgestaltung im nationalen und europäischen Kontext, CR 3/2012, S. 204ff.

이러한 정부규제의 한계를 보완하려면, 개인정보를 처리하는 기업의 협력과 자발적 준수가 요청된다. 개인정보의 '보호'를 개인정보를 이용하는 모든 프로세스에 내재화(privacy by design & default)하고 개인정보보호법의 규제 목적과 취지에 맞게 스스로 자율규제 규약(code of conduct)을 제정하여 준수함으로써 정부규제의 결함을 메우고 한계를 뛰어넘을 수 있다. 기업의 협력과 자발적 준수를 넓은 의미에서 자율규제라고 보면, 정부규제와 자율규제의 협력과 조화가 개인정보보호 규제의 실효성을 높일 수 있는 것이다.[2)]

이러한 개인정보보호 자율규제는 사회적 가치와 밀접한 관련이 있다. 문재인 정부의 국정과제로도 제시되어 있으면서 국회의 제도화 노력으로 이어지고 있는 사회적 가치의 개념은 "경제 뿐만 아니라 사회·환경·문화 등을 포함하는 영역에서 공공의 이익과 공동체의 지속가능한 발전에 기여하는 핵심가치"를 의미한다.[3)] 특히 우리사회가 우선적으로 추구해야 할 세부가치로 '윤리적 생산과 유통을 포함한 기업의 자발적인 사회적 책임 이행'이 제시되고 있다. 이를 기업의 사회적 책임(Corporate Social Responsibility)으로도 설명할 수 있는데, 그 구성요소 중 하나인 규범준수(Compliance)[4)]는 실제 자율규제라고 이해된다.[5)] 결국 자율규제는 사회적 가치를 구성하는 세부가치라고 할 수 있고, 개인정보보호 논의에 그대로 적용할 수 있다.

2) 자율규제를 규제완화로 오해하고, 개인정보보호의 자율규제를 정보처리자에게 유리한 체계로 인식하는 견해가 있을 수 있다. 하지만 자율규제는 규제를 완화하거나 규제를 포기하려는 것이 아니다. 규제를 합리화하는 것이다. 그리고 모든 개인정보보호 규제를 자율규제로 전환하고자 함이 아니라, 규제의 자원을 체계적으로 배분하여 중요한 규제는 국가에 유보하고 국가는 중요 규제에 집중할 수 있도록 하면서, 자율규제를 통해 일상적인 규제를 내재화하여(internalization) 정보처리자들이 스스로 개인정보보호 규제를 준수할 수 있도록 체계적 바탕을 마련해주고자 하는 의도이다. 이 글은 자율규제가 선언적이 아니라 '제도화'된 EU GDPR의 논의를 소개하는 시론적 성격이 강하며, 개인정보보호의 자율규제 안착을 위한 구체적인 제안은 추후의 연구과제로 남겨두기로 한다.

3) 관계부처 합동, 「사회적 가치 실현을 위한 공공부문의 추진전략」, 2020. 1. 15.

4) 이규영·곽재성, "기업의 사회적 책임(CSR) 개념의 재정립과 구조화", 사회과학연구 제41권 제3호, 2015, 121면.

5) 김재윤, "기업범죄예방과 관련하여 자율규제로서 준법인지원인제도의 이해 - 독일의 논의를 중심으로 -", 비교형사법연구 제21권 제3호, 2019, 61면 이하.

이와 같은 개인정보보호 자율규제 논의의 맥락과 사회적 가치 간 관계를 전제로, 이하에서는 EU의 개인정보보호 자율규제 체계를 소개함으로써, 사회적 가치의 세부가치인 자율규제를 우리나라에 활성화하기 위한 단초를 제공하고자 한다. 주지하다시피, EU의 개인정보보호를 위한 제도적 틀은 GDPR(General Data Protection Regulation)[6]이다. EU의 개인정보보호 자율규제는 결국 GDPR에서의 개인정보보호 자율규제제도이다.

2. EU의 개인정보보호 자율규제

(1) 개인정보보호 자율규제의 유형

EU GDPR의 공식적이고 직접적인 자율규제의 법적 근거는 ⅰ) 제40조의 자율규제 규약(Code of Conduct)과 ⅱ) 제42조의 인증(Certification)이다. 자율규제의 수단으로 명시되어 있지는 않지만, 개인정보보호담당관(Data Protection Officer)을 규정하고 있는 ⅲ) 제37조 이하의 규정도 실질적으로 자율규제의 수단으로 볼 수 있다.

(2) 자율규제 규약

자율규제 규약은 협회 또는 대표단체가 규약(안)을 제출하여 개인정보보호 규제당국의 승인(approve)을 받음으로써 GDPR에서 예정하는 규범적 효력이 발생한다. 자율규제 규약의 내용은 개인정보 수집, 개인정보 가명화, 정보주체의 권리행사 등 GDPR의 규제를 '구체화'한 것이다(GDPR 제40조 제2항). 개인정보보호 자율규제의 기능 중 하나는 개인정보가 이용되는 영역의 특수성이 고려된 섬세한 규율, 기술의 발전에 대한 적시 대응과

6) Regulation (EU) No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016), OJ L 119, 1.

불확정 개념의 구체화가 가능하다는 점이다.[7] 이로써 개인정보처리자에게 상당한 법적 안정성이 부여되는 효과가 있다. EU 회원국에서는 광고·보험·위치정보·금융분야 등의 자율규제 규약이 승인되어 시행되고 있다.

자율규제 규약의 승인 효력은 자율규제 규약의 규범력을 뒷받침하기 위한 중요한 전제이다. 개인정보보호 규제당국은 제출된 자율규제 규약(안)이 EU의 개인정보보호 규제인 GDPR에 부합하는지를 심사한다. 이러한 승인 심사는 자율규제 규약과 GDPR 규제의 견련성(牽聯性)을 잘 드러낸다. 승인된 자율규제 규약은 규제당국이 공식 확인한 GDPR 규정의 해석기준이다. 규제당국은 행정의 자기구속(Selbstbindung der Verwaltung) 법리에 따라 자신이 승인한 자율규제 규약의 내용에 구속된다.[8] 최소한 개인정보처리자의 자율규제 규약 준수는 GDPR 규제 준수에 대한 추정적 효력이 부여된다. 자율규제 규약 준수는 GDPR에서 요구하는 요건의 충족을 입증하기 위한 요소로 원용될 수 있는 것이다.[9] 자율규제는 법적 근거 없이도 시행될 수 있으나, 자율규제의 명문화는 자율규제에 더욱 권위와 힘을 실어주는 것이다.

(3) 인증

인증도 자율규제 규약과 함께 GDPR의 대표적인 자율규제의 수단이다. 다만, 자율규제 규약은 GDPR 규제를 구체화하는데 기여하는 반면, 인증은 인증받은 개인정보처리가 GDPR 규제를 실제로 준수하였음을 증명하기 위한 목적이 더 크다. 이로써 개인정보처리자의 GDPR 규제 준수를 더욱 제고할 수 있으며, 개인정보를 활용하는 제품 및 서비스의 개인정보보호 수준을 빠르게 조망해 볼 수 있다.

인증은 다음과 같은 GDPR 규제의 준수를 증명하기 위해 원용된다. GDPR 제24조 제3항

7) Matthias Bergt, Art. 40, in: Kühling/Buchner, DS-GVO·BDSG Kommentar, 2. Aufl., 2018, München, S. 765.

8) Matthias Bergt, a.a.O., S. 778, Rn. 41.

9) GDPR 제24조 제3항; 제28조 제5항; 제32조 제3항.

에 따른 기술적·관리적 조치 의무 준수를 인증으로 입증할 수 있다. GDPR 제25조 제3항은 인증을 개인정보보호 내재화(privacy by design & default) 의무를 준수했다는 증명 요소로 보고 있다. GDPR 제28조 제5항과 GDPR 제32조 제3항도 이와 같은 인증의 규범적 효력을 규정하고 있다. 인증을 받은 개인정보처리자에게 개인정보처리를 위탁하는 위탁자는 개인정보를 처리하는 수탁자의 GDPR 규제 위반에 따른 책임을 부담할 리스크가 상대적으로 완화된다. 인증을 받은 하드웨어나 소프트웨어를 공급하면 개인정보보호 내재화 설계로 제작되었기 때문에, 이를 이용함에 따른 책임이 줄어들 수 있게 된다.

(4) 개인정보보호담당관

독일의 개인정보보호담당관(Datenschutzbeauftragter)은 1977년 제정된 독일 연방개인정보보호법(Bundesdatenschutzgesetz, BDSG)에서 처음으로 도입되었다. 독일에서는 개인정보를 처리하는 민간을 국가가 규제하는 것은 헌법상 문제가 있다는 인식이 있었다. 민간영역에 대한 독립 규제기관의 규제는 엄청난 반대에 직면하였고 그 대안으로 개인정보보호 규제는 자율규제에 맡겨졌던 것이다.[10] 이에 따라 독일의 개인정보보호 규제는 2단계 통제시스템으로 설계되었다. 1차적으로는 개인정보처리자의 내부 개인정보보호담당관이 규제를 담당하였고, 외부 규제기관은 2차적으로 엄격한 조건 하에 개입하도록 체계화되었다. 다만, 개인정보보호담당관은 국가의 규제를 대체하는 것은 아니고, 국가의 규제를 보충하고 국가의 규제부담을 경감하는 기능을 수행한다. 개인정보보호담당관은 내부 통제기관으로서 개인정보처리자로 하여금 개인정보보호 규제를 준수하도록 지원하는 것이다.

개인정보보호담당관은 '개인정보처리가 행정청 또는 공공기관에 의해 수행될 경우', '개인정보처리자의 핵심적인 활동 영역이 정보주체로 하여금 포괄적이고 주기적인 감시가 요구되는 경우', '개인정보처리자의 핵심적인 활동 영역이 민감정보 또는 형사상의 유죄

10) 개인정보보호담당관은 개인정보보호법에서 자율규제의 핵심적인 요소라는 견해는 Matthias Bergt, Art. 37, in: Kühling/Buchner, DS-GVO·BDSG Kommentar, 2. Aufl., 2018, München, S. 715.

판결 및 범죄행위와 관련된 개인정보를 대규모로 처리하는 경우'에 반드시 지정되어야 한다(GDPR 제37조 제1항). 개인정보보호담당관은 개인정보보호처리자 및 그 업무 종사자에 대해 GDPR 규제의 교육 및 자문, GDPR 준수에 대한 감독, 개인정보영향평가에 대한 자문 및 평가, 규제당국과의 협업, 개인정보처리와 관련된 문제의 처리를 위한 규제당국의 소통창구로서 역할을 수행한다(GDPR 제39조). 이러한 개인정보보호담당관의 기능과 이를 지정할 의무로부터 개인정보보호위원 제도가 개인정보보호 규제의 핵심적인 수단임을 알 수 있게 한다.[11)]

3. 개인정보보호 자율규제의 활성화 과제

EU GDPR의 개인정보보호 자율규제는 '규제의 견련을 통한 규범력 및 인센티브 고양, GDPR 규제 준수의 증명으로 활용, 사전예방적 내부 자율준수체계'라는 특징이 있다. 자율규제의 이러한 특성이 자율규제의 활성화 요인으로 작용할 수 있는 것이다. 그렇다면 우리의 개인정보보호 자율규제를 활성화하기 위한 과제는 무엇인가?

(1) 선결문제

개인정보보호 자율규제의 활성화를 논하기 이전에 사회적 가치를 고양하는 수단인 개인정보보호 자율규제로부터 무엇을 기대할 수 있는지부터 따져야 한다. 일반적인 개인정보보호 자율규제의 장점은 자율규제체계의 전문성, 개별 영역별 특수성 고려, 규제기관의 부담경감 등이다. 다음으로, 이러한 기대를 충족하는데 우리나라 현행의 자율규제질서에 대한 체계적인 분석평가와 반성이 필요하다. '우리의 자율규제체계는 이러한 목적과 기능에 충분한가? 부족한 점은 없는가? 그 원인은 무엇인가?'에 대한 분석과 평가가 선행될 필요가 있다.

11) Stefan Eßer/Nils Steffen, Zivilrechtliche Haftung des betrieblichen Datenschutzbeauftragten Wann haften interner und externer Datenschutzbeauftragter? CR 5/2018, S. 289ff(290). 독일에서는 개인정보보호담당관이 개인정보보호 규제에 있어 핵심적이라고 하고 있지만, GDPR에서는 이러한 핵심적인 역할이 독일에 비해 축소되었다고 한다.

이 외에도 '우리의 개인정보보호 규제조직은 충분한 규제역량으로 최소한 현행 규제의 실효적 집행을 뒷받침하고 있는가? 현실적으로 개인정보처리자는 얼마나 많은가? 이들에 의해 처리되는 개인정보의 양은 또 얼마나 많은가?' 등의 질문들에 대한 숙고도 함께 이루어져야 한다.

이러한 통찰과 고민의 과정 끝에 개인정보보호 자율규제의 가치, 필요성, 현행 자율규제 체계의 문제점들이 드러날 것이다.

(2) 자율규제의 합리적 활용 범위

개인정보보호 자율규제는 국가의 규제와 병존이 불가피하다. 그렇다면 자율규제로 맡길 업무의 범위를 결정해야 한다. 자율규제에 적합한 업무는 감독보조적 기능으로서, 일상적·반복적 기능적 성격의 규제업무, 규제기관의 인적·물적 능력의 한계로 인하여 직접 영위하기 어려운 업무, 자율적 질서형성이 요구되는 영역의 규제기능[12], 규제기관이 직접 규제하는 것이 기업 경영에 간섭을 야기하여 기업의 자유와 창의를 억제하게 될 우려가 있는 규제기능 등이다. 자율규제의 업무범위를 결정하기 위해서는 현행 국가의 규제와 자율규제체계에 대한 진단이 선행되어야 할 것이다.

(3) 한국의 개인정보보호 자율규제

가. 자율규제 규약

개인정보보호법은 개인정보보호 자율규제의 활성화(법 제9조 제2항 제4호)와 자율규제의 촉진 및 지원(법 제13조) 규정을 두고 있다. 자율규제의 촉진 및 지원 시책으로 교육·홍보, 개인정보보호 관련 기관·단체의 육성 및 지원, 인증마크도입·시행 지원, 규약 제정·

12) 즉, 당해 영역의 구체적인 질서가 국가의 입법자에 의해 정해지기 보다 당사자들이 자율적으로 정하는 것이 타당한 영역, 예컨대, 전문적 영역, 전문적인 특정집단을 규율대상으로 하는 규제 등을 고려해 볼 수 있다.

시행 지원 등을 열거하고 있다. 한편, 방송통신위원회는 2018년 3월에 「정보통신서비스 분야 개인정보보호 자율규제 기본계획」을 수립한 바 있다. 이에 따른 자율규제 단체로는 한국온라인쇼핑협회, 한국정보통신진흥협회, 한국알뜰통신사업자협회, 한국게임산업협회, 한국케이블TV방송협회, 한국IPTV방송협회, 한국인터넷기업협회, 개인정보보호협회 등이 있다.

우리나라도 자율규제의 준수에 따른 인센티브를 부여하고 있다. 「자율규제단체 지정 등에 관한 규정」 제15조의2에 따르면, 자율규제단체의 자율규제 활동에 참여하는 소속 개인정보처리자가 자율규제 규약을 충실히 준수하고 자율점검을 성실히 수행하여 수행결과가 우수하다고 인정되는 경우 자료제출 및 검사는 1년간 면제할 수 있음을 규정하고 있다. 다만, 개인정보처리자가 개인정보보호법을 위반하였거나 그 혐의가 있을 경우는 제외한다.

문제는 이러한 인센티브가 개인정보처리자를 '자발적'으로 자율규제시스템에 편입시키기 위한 충분한 유인책인지 여부이다. 또한, 자율규제를 촉진 및 지원하기 위한 시책의 근거를 마련해두고 있어 유연한 자율규제체계의 구축이 가능한 것으로 보이지만, 반대로 예측가능성과 법적 안정성이 결여되어 있어 어떠한 촉진·지원책이 있는지, 이에 따를 때 어떠한 혜택이 부여되는지에 대한 불확실성이 존재한다.

나. 인증

한국의 인증제도는 정보보호 및 개인정보보호 관리체계 인증인 'ISMS-P'이다. 인증제도의 법적 근거는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 (이하 '정보통신망법') 제47조, 제47조의3 및 개인정보보호법 제32조의2이다. 이전에는 정보보호 관리체계 인증인 ISMS와 개인정보보호 관리체계 인증인 PIMS가 별도로 존재하였는데, 이를 ISMS-P 체계로 단일화하였다.

ISMS-P를 취득한 경우 인센티브는 방송통신위원회의 「개인정보보호 법규 위반에 대한

과징금 부과기준」 [별표]에 따른 추가적 과징금 감경(50%)이다. 명시되어 있지는 않지만 규제 위반에 따른 형사절차에서 고의·과실 판단 시 참작 정도를 좌우하는 요소로 작용한다.

문제는 EU의 GDPR과 같이 전적으로 자율에 의존하는 체계는 아니라는 점이다. 정보통신망법 제47조 제2항은 인증 의무대상자를 규정하고 있다. 또한, EU의 GDPR처럼, 인증 취득 시 법준수(합법성)의 추정효 등을 실무적으로 인정하고 있는지에 대해서도 불분명하다. 과징금의 감경사유나 고의·과실 판단 시 참작 사유 정도로 국한된다. 개인정보보호법 제32조의2는 인증의 내용을 표시하거나 홍보할 수 있는 인센티브만 부여하고 있으며, 인증을 받지 않았음에도 불구하고 거짓으로 인증의 내용을 표시하거나 홍보하는 자에 대한 과태료 부과 근거만 규정하고 있다(법 제75조 제2항 제7의2호).

다. 개인정보보호담당관

우리나라에서 EU GDPR의 개인정보보호담당관(DPO)과 동일한 제도는 존재하지 않는다. 다만, 이와 유사한 개인정보보호법의 개인정보 보호책임자(Chief Privacy Officer, CPO)와 정보통신망법의 정보보호 최고책임자(Chief Information Security Officer, CISO) 제도를 두고 있다. CPO의 임무는 개인정보 보호계획 수립·시행, 처리실태 및 관행의 정기조사·개선 불만처리 및 피해구제, 내부통제시스템 구축, 교육계획 수립·시행,파일의 보호·감독, 법위반 시 개선조치 등이다. CISO의 임무는 정보보호관리체계 수립 및 관리·운영, 정보보호 취약점 분석·평가 및 개선, 침해사고 예방 및 대응, 사전 정보보호 대책 마련 및 보안조치 설계·구현 등, 정보보호 사전 보안성 검토, 중요 정보의 암호화 및 보안서버 적합성 검토 등의 업무 등이다.

CPO와 CISO는 EU GDPR의 개인정보보호담당관(DPO)과는 지위, 임무, 자격 등이 상이하지만, '내부통제시스템 구축', '사전 정보보호대책 마련', '정보보호 사전 보안성 검토' 등은 DPO와 마찬가지로 사전예방적 내부 자율준수 체계를 염두에 둔 제도로 볼 수 있다. 그러나 우리의 현재 법실무에서는 기업 내부에서의 독립성, CPO와 CISO에 대한 책임의 과중함, CPO와 CISO간 업무의 중첩 등의 문제가 지적되고 있다. 이러한 상황에서 추가

적으로 EU GDPR의 개인정보보호담당관 제도 도입도 검토되고 있는 단계이다. 개인정보보호담당관 제도의 도입이 필요한지 여부에서부터, 기존의 CPO 및 CISO와의 관계, 이들 제도가 추구하는 사전예방적 내부 자율준수 체계의 실효성 제고방안을 포괄하는 신중한 검토가 필요한 시점이라고 본다.

(4) 향후 과제

우리나라도 개인정보보호 자율규제체계가 작동하고 있음에도 불구하고, 자율규제가 활성화되어 있다고 평가하기 어려운 상황이다. 자율규제를 활성화하기 위해서는 무엇보다 실효적인 자율규제의 인센티브를 고민해야 한다. 자율규제의 인센티브로 개인정보보호 규제의 준수에 대한 추정효 부여와 규제와의 견련성이 유력하게 검토되어야 할 것이다. 또한, 규제기관과 자율규제기관의 협업이 필요하다. 사전예방적 내부 자율준수체계가 정착될 수 있도록 CPO와 CISO 제도에 대한 평가와 이에 기초한 제도개선이 필요하다.

KOREA LEGISLATION RESEARCH INSTITUTE

KLRI

IV

개인정보와 현행 이슈들

01 프라이버시의 사회적 가치를 생각하는 윤리적 연구

오철우 강사 (서울과학기술대학교)

1. 들어가는 말

개인 유전체 정보는 아데닌, 구아닌, 티민, 시토신, 이렇게 네 염기(A, G, T, C)의 수없는 반복으로 구성된다. 이런 개인 유전체의 염기서열 정보가 누구 것인지를 익명 처리하면 그 주인의 신원을 식별하는 건 불가능할까? 익명 처리를 한다 해도 유전체의 특정 부분 정보를 분석하고 또 유전자 계통도 데이터베이스를 검색해 비교하는 몇 가지 단계를 거치고, 다시 인터넷에서 찾을 수 있는 일반 정보들과 조합하면, 놀랍게도 유전체 정보의 주인을 비교적 높은 확률로 찾아낼 수 있었다고 한다. 2013년에 과학저널《사이언스》에 발표된 논문의 연구결과인데,[1] 이 논문은 당시에 별문제 없다고 생각했던 개인 유전체 정보의 공유 시스템에 경각심을 불러일으킨 계기가 됐다. 논문을 낸 미국 생물정보학 연구진은《네이처》의 뉴스보도에서 발표를 망설이다가 이런 공개 발표가 시스템의 결점을 세상

1) Melissa Gymrek et al., "Identifying Personal Genomes by Surname Inference," Science 339, 18 January 2013, pp. 321-324; 오철우, "익명의 게놈 개인신원 확인 잇따라, 프라이버시 경고음", 한겨레《사이언스온》, 2013. 5. 14. http//scienceon.hani.co.kr/100153"http://scienceon.hani.co.kr/100153 (최종방문일 2020. 7. 7.)

에 알려 경고하고 궁극적으로 과학을 강화하는 데 기여할 것으로 믿었다고 말했다.[2] 같은 해에 미국 하버드대학 연구자는 유전체 정보에 붙은 성별, 출생일, 우편번호 같은 조각 정보를 이용하고 인터넷 검색 정보와 결합해 579명의 유전체 정보에서 241명의 신원을 식별했으며 그 정확도는 84~97%에 달했다고 보고했다.[3]

과학기술의 발달로 전에 없던 새로운 성격의 개인정보들이 만들어지고 저장되고 전송되고 사용된다. 개인 유전체 정보는 점차 다양한 의료 서비스에서 활용되며, 사람들의 소비, 이동, 행동을 기록하는 개인 생활 데이터가 갖가지 스마트 기기와 인공지능을 작동하는 데 활용된다. 인체와 기계를 연결하는 여러 첨단 기기는 개인 생체정보를 활용해 작동된다. 이런 새로운 성격의 개인정보들을 활용하는 신기술의 연구개발이 늘면서, 과학기술계에서도 개인정보의 안전성과 프라이버시와 관련한 논의와 관심도가 높아지고 있다.

2. 유전체학, 신경공학, 인공지능의 프라이버시 논의

과학기술 연구에서 프라이버시 이슈는 대량의 데이터 생성과 저장, 공유 기반이 발전하면서 빅데이터와 맞춤형 정보를 활용하는 기술 영역이 확장하는 흐름과 함께 등장했다. 이 가운데, 대량의 개인 유전체(퍼스널 게놈) 정보를 다루는 유전체학 분야에서 프라이버시 이슈는 비교적 일찍부터 제기되었다. 다량의 개인 유전체 정보가 인류 기원이나 민족 집단 이동 연구에 사용되거나 인구집단의 건강과 질병에 관한 유전체 기반의 역학연구에 활용되기도 하는데, 근래에는 맞춤형 의료의 기반으로 다양하게 응용되면서 개인 유전체의 프라이버시 문제가 꾸준히 논의되고 있다.

그 중에 관심의 초점이 되는 것은 개인별 유전자 검사 서비스이다. 2020년 6월《네이

2) Erika Check Hayden, "Privacy protections: The genome hacker," Nature 497, 9 May 2013, pp. 173-173.

3) Latanya Sweeny et al., "Identifying Participants in the Personal Genome Project by Name," arXiv:1304.7605 [cs.CY]. https://arxiv.org/abs/1304.7605?utm_source=feedly (최종방문일 2020. 7. 7.)

처 제네틱스》에 실린 논문은 개인 유전체를 둘러싼 프라이버시 논란의 현주소를 보여준다. 논문 저자인 미국 샌디에이고 캘리포니아대학 연구진은 유전체 데이터의 생산과 저장, 공유의 비용이 점점 낮아지면서 프라이버시 문제의 범위가 확장하고 있다며 그 실태를 지적했다.[4] 특히 상업 서비스로서 개인별로 유전자를 검사해주는 이른바 '소비자 직접 의뢰(DTC: Direct to Consumer)' 유전자 검사 서비스가 늘면서, 개인 유전체 정보의 오남용 문제는 일반 시민 생활로 확장하고 있다고 지적된다. 건강과 질병, 그리고 유전형질 정보를 담은 유전체 프라이버시 문제는 당사자 개인뿐 아니라 친족과 후손의 프라이버시에도 영향을 줄 수 있다.

이 연구진은 그동안의 유전체 프라이버시 침해 사례와 연구를 종합해, 유전자 프라이버시 침해가 두 갈래 유형으로 일어난다고 분석했다. 하나는 공격자가 특정 유전체 정보를 분석하고 인터넷의 여러 정보와 결합하는 방식으로 그 유전체가 누구의 것인지를 식별할 수 있으며(신원 식별), 다른 하나는 특정인 ㄱ씨의 유전체 정보 일부를 이용해 유전체 공유 데이터베이스에서 ㄱ씨의 유전체 정보 전체를 찾아내어 개인의 생물학적, 유전적 특성 전체를 파악할 수 있다는 것이다(표현형 식별). 실제로 미국에서는 DTC 유전자 검사 서비스 기업들이 다량의 개인 유전체 데이터베이스를 갖추고 있는데, 경찰이 범죄 현장에서 확보한 유전체 일부 정보를 이런 DTC 유전자 데이터베이스를 통해 범인을 식별해내어 찾아낸 사례들이 있었다. 이런 사례는 유전체 식별 기술이 공공적 목적이 아니라 다른 목적으로 오남용되거나 악용된다면 개인의 유전자 프라이버시가 언제든 침해될 수 있음을 또한 보여준다.

몸을 움직이지 못하는 환자를 위해 로봇팔 같은 신경계 대체 기구를 개발하는 신경보철(neuroprosthetics) 분야에서도 프라이버시 이슈가 제기된다.[5] 신경보철 기구는 뇌 또는

4) Luca Bonomi et al., "Privacy challenges and research opportunities for genomic data sharing," Nature Genetics 52, 2020, pp. 646-654.

5) Jens Clausen et al., "Help, hope, and hype: Ethical dimensions of neuroprosthetics," Science 356, 30 June 2017, pp.1338-1339.

신경계와 주고받는 생체신호와 전자신호에 의해 작동하는데, 이때 무선으로 오가는 신호의 안전성과 프라이버시는 중요한 문제가 된다. 누군가가 무선 인터페이스에 침입해 개인정보가 되는 데이터를 낚아채거나 더욱 위험하게는 환자의 뇌나 신경계, 또는 보철기구에 위험한 신호나 명령을 주입할 수 있기 때문이다. 작동원리로 볼 때 개인 생체정보를 들여다보거나 신경계에 개인의 의지와 상관없이 다른 신호를 집어넣는 게 불가능하지 않다. 이런 점에서 신경공학 분야에서는 안전성과 프라이버시가 동전의 양면과 같은 문제로 받아들여진다.

신경공학에서는 뇌와 기기를 연결해, 뇌에 좋은 자극을 주거나 인지 기능을 증강하려는 인터페이스 기술의 개발과 사용이 늘고 있는데,[6] 마찬가지로 공격자가 인터페이스를 해킹해 사용자의 뇌에 영향을 주는 신호에 개입하거나 사용자의 감정, 마음 상태와 관련한 데이터를 가로채 엿볼 수 있다는 안전성과 프라이버시 문제가 일찌감치 제기되어 왔다.[7] 이와 다른 분야이지만 뇌기능 자기공명영상(fMRI)을 거짓말 탐지기 같은 기능으로 활용하려는 시도와 관련해, 뇌영상이 규제 없이 사용될 때 '뇌 프라이버시'가 훼손될 수 있다는 우려도 오래전부터 제기되어 왔다.

요즘에 가장 활발한 프라이버시 논의는 인공지능 분야에서 이뤄지고 있다. 인공지능 기술은 환경 감지와 인간사회 활동에서 생성되는 갖가지 빅데이터에 기반을 두어 작동하기 때문에, 여러 윤리 이슈 중 하나로서 프라이버시 문제는 인공지능 기술이 마주해야 하는 고유한 문제로 다뤄져 왔다. 인공지능의 개발과 사용에서 강조되는 윤리적 원칙은 대

6) 연합뉴스, "페이스북, '뇌 · 피부-컴퓨터 인터페이스' 개발 중", 2017. 4. 20. https://www.yna.co.kr/view/AKR20170420031500091 (최종방문일 2020.7. 7.); 연합뉴스, "머스크의 다음 실험은 '인간 뇌-컴퓨터 연결 기술'…내년 목표", 2019. 7. 17. https//www.yna.co.kr/view/AKR20190717156600009"https://www.yna.co.kr/view/AKR20190717156600009 (최종방문일 2020. 7. 7) 신경공학의 이런 인터페이스 기술은 Brain-Machine Interface[BMI], Brain-Computer Interface[BCI], Mind-Machine Interface[MMI] 등으로 불린다.

7) Tamara Denning et al., "Neurosecurity: security and privacy for neural devices," Neurosurg Focus 27 (1): E7, 2009.

표적으로 2019년 경제협력개발기구(OCED) 보고서와 주요 20개국(G20) 통상무역 및 디지털경제 분야 장관회의에서 제시한 '사람 중심 인공지능(Human-centered AI)'에서 확인할 수 있다.[8] 주요한 인공지능 원칙을 보면, 편향과 차별이 없는 인공지능의 '공정성' 원칙, 예측, 권고, 판단의 근거와 합리성을 인간에게 설명할 수 있는 인공지능과 같은 '투명성'과 '책임성', '설명가능성'의 원칙과 더불어, 프라이버시와 정보보안을 지키면서 빅데이터를 사용하는 인공지능의 '프라이버시 존중' 원칙이 중요하게 다뤄진다.[9]

눈에 띄는 점은 '인간 중심의 인공지능'이라는 표현에서 볼 수 있듯이, 이런 윤리 원칙이 사회의 신뢰성과 수용성을 높이기 위해서 먼저 갖춰야 하는 안전하고 지속가능한 기술의 '문턱' 기준으로 여겨진다는 것이다. 초고속 통신 기술을 바탕으로 더 많은 영역에서 더 많은 기기를 통해 인공지능에 광범위하고 다양한 데이터를 제공하는 사물인터넷(IoT) 기술에서도 당연히 프라이버시는 매우 중요한 이슈이다.

프라이버시와 관련한 다양한 문제들은 더 많은 개인 데이터를 빅데이터로 저장하고 빠르게 전송해 활용할 수 있는 시대에, 염기서열이나 생체신호, 또는 일상생활 패턴 데이터처럼 개인정보로 변환할 수 있는 새로운 성격의 데이터 생성과 수집 방식이 발전하면서 새롭게 생겨나고 있다. 새로운 프라이버시 이슈가 새로운 기술과 함께 등장하는 것이다. 이 때문에 빅데이터의 시대에는 연구개발 단계에서 프라이버시 문제를 살펴보며 대안과 우회의 길을 찾는 윤리적 연구의 필요성이 함께 커진다.

8) OECD, Artificial Intelligence in Society, OECD Publishing, Paris, 2019.

9) Anna Jobin, Marcello Ienca and Effy Vayena, "The global landscape of AI ethics guidelines," Nature Machine Intelligence vol. 1, September 2019, pp.389-399.

3. 프라이버시와 연구윤리, 윤리적 연구

연구자가 연구대상자 또는 연구참여자의 개인정보를 보호해야 한다는 것은 오래전부터 강조되는 연구윤리 규범이다. 일례로, 연구자는 연구 중이나 이후에 개인정보 유출을 막고 기밀을 유지해야 하며, 연구참여자의 추가 동의를 받지 않았다면 개인정보를 연구 외에 다른 목적으로 사용하지 말아야 한다.

이런 규범은 일찌감치 1993년 국제의과학기구협의회(CIOMS)와 세계보건기구(WHO)가 발표한 인체 대상 의과학 연구의 윤리 가이드라인에 담겼다. 연구참여자의 프라이버시를 존중하고 개인정보 기밀을 유지해야 할 책임과 의무가 명시됐다. 이어 2005년 10월 유네스코(UNESCO) 총회에서 발표된 생명윤리와 인권에 관한 보편선언에서도 프라이버시와 기밀성 조항은 프라이버시 존중과 개인정보 기밀 유지를 강조하고 정보를 수집한 목적과 합의된 목적 외에 사용하거나 유출해서는 안 된다고 규정한다.[10)]

국내의 연구윤리 규범에서도 마찬가지다. 교육부 훈령으로 제정된 「연구윤리 확보를 위한 지침」[11)]을 보면, 연구자가 지켜야 하는 열 가지 사항 중 하나로 “연구대상자의 개인정보와 사생활 보호”가 열거되었다(제5조 제2호). 구체적인 지침은 전문 분야별로 규정되었는데, 예를 들어 국가생명윤리정책원이 운영하는 기관생명윤리위원회(IRB)의 정보 포털에는 「생명윤리 및 안전에 관한 법률」(이하 ‘생명윤리법’)에 따른 「개인정보보호 지침」을 따로 자세히 마련해 두었다. 이에 따르면 인체 유래물 은행에서는 기증자를 식별할 수 없도록 익명으로 처리해야 하고, 기증자 개인정보의 보안책임자를 따로 지정하도록 했다.[12)]

10) 권복규·김현철, 『생명 윤리와 법』, 이화여자대학교출판부, 2009, 37-38면.

11) [시행 2018. 7. 17.] [교육부훈령 제263호, 2018. 7. 17., 일부개정].

12) 기관생명윤리위원회 정보포털, “정보관리 및 개인정보보호”, 국가생명윤리정책원. https://www. irb. or.kr/UserMenu06/PreservationInfomationManagement.aspx (최종방문일 2020. 7. 7.)

연구윤리 규정들은 연구자의 역할과 책임을 다하는 연구 활동을 독려하고 일탈을 막기 위한 지침으로 제시된다는 특징을 지닌다. 본래 연구윤리의 중심 관심사는 연구 결과의 신뢰성을 보증하기 위해서는 정직하고 진실한 연구 과정을 거쳐야 한다는, 이른바 '연구 진실성'의 추구에 초점을 맞춘다. 그러므로 연구대상자 또는 연구참여자의 프라이버시와 개인정보보호는 연구진실성을 추구하는 연구자가 연구 과정에서 지켜야 하는 윤리적 규범의 하나로 받아들여진다.

프라이버시 보호의 사회적 가치를 강조하는 과학기술계의 흐름은 연구 과정의 연구윤리 규범을 확장해, '과학기술의 사회적 책임'을 생각하는 윤리적 연구의 차원에서 이해할 수 있다. 예컨대 연구자가 연구진실성을 추구하는 연구윤리 규범을 성실히 지켰더라도 연구 결과물이 뜻하지 않게 부정적인 사회적 영향을 초래할 수 있으므로, 연구자는 이에 대해서도 책임감을 지녀야 하고 이런 책임감을 연구 과정에 반영해야 한다는 것이다.
예컨대 공학 분야의 대표적인 윤리 가이드를 보면, 사회적 가치를 지키려는 책임감 있는 연구 활동으로서 사회적 책임이 강조된다.[13] 과학기술이 사회에 끼치는 영향이 넓어지고 커지면서, 과학 연구 경쟁의 가속화, 과학 연구의 상업화 같은 요인으로 인해 과학기술의 사회적 책임이 강조되는 지금 시대에 연구실 안의 연구윤리를 넘어서서 사회와 소통하고 조화하는 윤리적 연구의 필요성이 더욱 부각된다. 이런 점에서 연구자는 자신의 연구에 대해 정직해야 할 뿐만 아니라 그 연구가 가져올 잠재적인 영향에 대해서도 숙고하고 이에 대해서 시민사회와 대화할 필요가 있다.[14]

요즘에는 '윤리적인 인공지능'이나 '윤리적인 로봇'과 같은 표현처럼 특정 과학기술의 이름과 윤리의 수식어를 결합한 신조어를 자주 볼 수 있다. 그만큼 과학기술의 사회적 책임이 강조되며, 또한 기술의 설계와 연구개발 과정에 윤리적인 고려를 반영해야 한다는 의

13) "IEEE Code of Ethics," IEEE Policies. https://www.ieee.org/about/corporate/governance/p7-8.html.

14) 홍성욱, "연구윤리의 사회적 맥락", 이상욱·조은희 엮음, 「과학 윤리 특강 -과학자를 위한 윤리 가이드」, 사이언스북스, 2011, 65-85면.

미로 받아들여진다. 여기에서 프라이버시 보호라는 윤리적 연구의 문제로 바라본다면, 연구자의 연구진실성 차원의 프라이버시 보호 지침을 이행하는 문제와는 별개로, 연구자가 프라이버시를 보호를 위한 대안의 기술을 모색하거나 기존 기술에서 프라이버시와 관련한 부분을 보완하는 연구에 나서는 윤리적 연구 활동도 주목을 받기 시작했다고 말할 수 있다.

사회적 가치를 생각하는 과학기술은 기술 혁신이 성공적인 방향으로 나아가기 위해서는 기술과 사회가 소통하며 함께 혁신해야 한다는 인식에 바탕을 두고 있다. 이런 분위기에서 "과거에는 기술 발전과 비즈니스가 윤리와 갈등 관계에 있었던 반면, 인공지능의 발전은 도리어 윤리를 고려해야 기술 발전과 비즈니스가 가능한 사회로 우리를 이끌고 있다"는 인식도 널리 받아들여진다.[15)]

윤리적 접근은 사회적으로 허용되거나 선호되는 가치를 제시해 적정한 기술 개발을 돕고, 법적으로 문제가 없더라도 사회적 저항이 큰 요소를 미리 판단해 기술 개발의 실패를 피하거나 줄일 수 있게 해준다는 점에서, '조기경보 시스템' 같은 역할을 할 수 있다.[16)] 빅데이터의 시대에 프라이버시 보호를 비롯해 여러 윤리적 쟁점을 극복하거나 우회하는 윤리적인 기술을 연구개발 하기 위해서는 다양한 분야가 참여하는 융합적인 노력이 연구개발 초기 단계부터 고려되어야 할 것이다. 연구윤리 지침이 아니라 윤리적인 기술을 지향하기 위해서는 창조적인 연구개발 활동의 주체인 연구자들 사이에서 프라이버시 감수성을 높이는 노력이 필요하다.

많은 기술이 이미 개인정보의 빅데이터를 다루고 있다. 강력해진 컴퓨터, 클라우드 플랫폼, 그리고 머신러닝 분석틀은 빅데이터를 처리하고 공유하는 틀이 된다. 유전체 기반의

15) 김효은, 『인공지능과 윤리』, 커뮤니케이션북스, 2019, 4면.

16) Luciano Floridi et al., "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations," Minds and Machines 28, 2018, pp. 689-701.

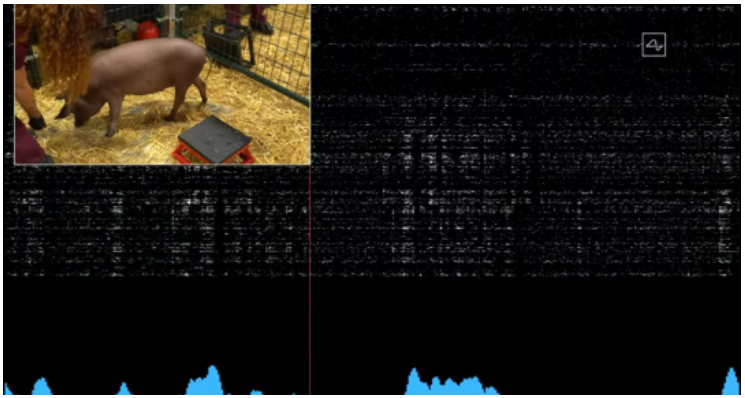
맞춤형 의료기술, 인공지능 기술, 로봇과 신경과학 같은 최신 기술이 이처럼 대량의 개인정보 없이는 작동하기 힘든 시대에 살고 있다. 이에 따라 과학기술 연구의 초기 단계에서 실용화 이후의 프라이버시 침해 문제를 고려해야 할 필요성이 제기되며, 또한 이런 프라이버시 문제를 회피하거나 넘어설 수 있는 대안의 연구개발 필요성도 덩달아 커졌다.

4. 맺음말

프라이버시는 우리의 인격과 자율적인 삶에 핵심으로서 중요한 인격적 가치이며, 또한 사회적 약자 보호를 비롯한 인권 보호, 그리고 민주적 의사결정과 참여라는 공공 이익과 공동체 발전을 위해 지켜야 하는 사회적 가치의 하나로서 인식되어야 한다. 최근에 국내에서도 이와 관련한 관심과 논의가 많아지는 것은 반가운 일이다.

흔히 과학기술은 중립적이기 때문에 신기술의 연구개발 과정은 이런 가치 논의와 거리가 멀다고 여겨지곤 한다. 하지만 혁신기술이 시장과 사회에 신뢰를 받으며 안착하기 위해서는 기술의 사회 진입과 확장 초기에 연구자뿐 아니라 사회의 여러 이해당사자들이 소통하며 사회적 가치와 조화를 이루는 기술 발전의 길을 모색해야 한다. 혁신기술의 성공을 위해서는 기술과 사회가 함께 혁신해야 하기 때문이고, 그것이 기술의 지속가능한 거버넌스를 가능하게 하기 때문일 것이다. 데이터를 활용하는 새로운 기술의 등장이 잦아지는 시대에, 개인정보와 프라이버시 보호는 실험실 안의 연구윤리 지침 중 하나가 아니라, 사회적 가치를 존중하는 윤리적 연구의 문제로 확장해서 바라봐야 하지 않을까 한다. 개인 데이터를 다루는 기술 분야의 연구개발 단계에서 프라이버시 감수성을 높이는 일이 중요하며, 이를 위해서 기술과 사회 간에 소통의 장이 넓어져야 하겠다.

팔다리가 마비된 환자가 뇌와 기계를 연결해 작동하는 로봇팔을 자신의 생각대로 제어하고 있다. 이런 뇌-기계 인터페이스(BMI) 기술에서도 데이터의 안전성과 프라이버시 보호 문제가 주요 이슈로 다뤄진다. 출처: 미국 피츠버그대학병원 제공(2012). 유튜브 화면 갈무리.



뇌-컴퓨터 인터페이스 기술을 개발하는 미국 기업 뉴럴링크가 2020년 8월 새롭게 개발한 뇌-컴퓨터 연결 칩을 시연했다. 위 영상은 이 칩을 이식한 실험동물 돼지가 킁킁 거리며 냄새를 맡자 그 뇌에서 생성되는 신호가 컴퓨터로 전송되어 화면에 나타나는 모습을 보여준다. 뉴럴링크 설립자인 일론 머스크는 개발중인 이 기술의 목표가 기억상실, 우울증, 불면증 등 다양한 신경학적 문제를 해결하는 데 도움을 주는 것이라고 밝힌다. 출처: 뉴럴링크(NeuralLink), 유튜브 화면 갈무리.

02 COVID-19와 프라이버시

이진규 이사 (네이버)

1. 들어가며

"K-방역"으로 대표되는 대한민국의 코로나19 대응은 감염병 예방 및 확산 방지 측면에서 상당히 효과적이라는 평가를 받았다. 2021년 2월 13일 0시 기준, 우리나라는 총 83,199명의 확진자를 기록했다. 겨울이라는 계절적 요인 등에 기인하여 한 때, 일일 확진자 수가 1,000명을 상회하기도 했으나 방역당국이 검사를 대폭 확대하여 감염재생산지수를 1 이하로 낮추는데 성공하기도 했다. 이는 전 세계 코로나19 통계 취합 대상 221개국 가운데 67번째로 낮은 수준이다. ▲Drive-Through 검사 ▲마스크 공적 판매 ▲자가 격리 어플리케이션 개발 ▲QR코드 기반 민-관 전자출입명부 운영 등 효과적이면서도 '우리만의' 독창적인 대응 기법들이 전 세계의 이목을 끌고 있다. 이에 고무된 정부는 전염병 대응 과정에서 '검사·확진→조사·추적→격리·치료'로 이어지는 18종의 절차와 기법을 <K-방역 3T(Test-Trace-Treat) 국제 표준화 분야>라는 명칭으로 국제표준화 할 계획을 밝히기도 하였다. 이러한 가시적 결과에도 불구하고, 감염병 환자의 이동경로(동선) 공개로 인한 세간의 억측과 사회적 낙인 등의 부작용은 공중보건과 안전의 이면에 프라이버시의 침해라는 폐해가 자리잡을 수 있다는 화두를 우리 사회에 던져주었다. 코로나19가 우리 사회에

던진 프라이버시에 관한 이슈를 살펴본다.[1)2)]

[표-3] K-방역 6개월 변천사 (출처: 뉴스1)

2월4일	코로나19 진단시약 1개 긴급사용승인 K-방역 시작점이면서 대량검사가 가능한 토대를 마련
2월9일	방역당국, 코로나19 하루에 소화할 수 있는 검사 건수 2월 말까지 1만건 확대 발표, 7월 현재 하루 최대 7만건까지 확대
2월10일	중국발 입국자 대상으로 증상 모니터링하는 애플리케이션(앱) 적용 발표 이후 자가격리 등으로 적용 분야 확대 최신 정보통신(IT) 기술 활용해 전 세계적으로 주목을 받음
4월7일	자가격리자 이탈 방지를 위해 전자손목밴드(안심밴드) 최초로 언급 4월 27일부터 본격 시행, 자가격리 애플리케이션(앱)과 연동
5월7일	전 세계 70개 국가에서 한국산 마스크 수입 요청 이후 100개국 이상으로 확대, 공적판매 개념 도입하고 5부제 통해 마스크 대란 극복
5월14일	K-방역 국제표준으로 만드는 내용의 '감염병 대응 산업 육성방안' 발표
5월31일	수도권 교회 감염 잇따르자 QR코드 기반 전자출입명부 시범 운영 6월 9일 주점 등 8개 고위험 시설에 의무 적용 이후 대형학원 등 고위험시설 4개 시설에 추가 적용 사나흘 걸리던 1000명 추적 기간을 하루로 단축하는 효과
6월16일	6차 K-방역 웹세미나 개최, 이날 기준으로 100여개 국가 2500여명에게 K-방역 노하우 전수

news1

1) Worldometer, “COVID-19 Coronavirus Pandemic”, https//www.worldometers.info/coro₩-navirus”https://www.worldometers.info/coro₩-navirus (최종방문일 2020. 9. 10.)

2) 뉴스1, “[코로나 6개월-③] 진단과 추적, 세계를 감동시킨 ‘K-방역’”, 2020. 7. 5. https:// news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=421&aid=0004735476 (최종방문일 2020. 9. 10.)

2. 이동경로 공개와 프라이버시 침해

"코로나바이러스보다 동선 공개가 더 무섭다." 이동경로 공개로 인한 신상공개 피해자들의 이와 같은 호소는 동선 공개가 정보주체의 프라이버시에 미치는 영향의 크기를 직·간접적으로 경험할 수 있게 한다. 2020년 2월 코로나19 확진 판정을 받은 한 남성이 식당에 들른 동선과 시간이 공개되었는데, 함께 식사를 한 사람이 '처제'라는 사실까지 밝혀지면서 둘 사이가 불륜이 아니냐는 의심을 받았다. 아내와 자녀는 음성판정을 받았는데, 처제만 양성 판정을 받자 루머는 눈덩이처럼 불어났다. 이동경로 공개는 2차 감염 피해를 줄이기 위한 목적에서 진행되는 것임에도 '식사를 함께 한 상대'와 '확진자의 관계'까지 과도하게 공개되는 바람에 이와 같은 논란이 발생한 것이다. 부산 온천교회 소속 남녀 확진자 2명은 비슷한 시간에 해운대구의 한 리조트에 머문 사실이 공개되자 인터넷에는 이들의 불륜을 의심하는 글들이 퍼져나갔다. 또, 새벽에 노래방 방문 동선이 공개된 한 20대 여성은 소위 '노래방 도우미'가 아니냐는 억측에 시달렸다. 급기야 "동선 공개로 사생활을 침해당했다"는 진정이 인권위원회 산하 부산 인권사무소에 제기됐으며, 최영애 국가인권위원회 위원장은 3월 9일자로 국가인권위원장 명의의 성명을 내어 "확진환자의 내밀한 사생활도 보호할 수 있는 방안을 강구할 필요가 있다."라고 주의를 촉구하였다. 온천교회 소속 남녀 확진자 2명의 경우, 부산시가 보도자료에 확진 번호를 잘못 기재한 사실이 있었다는 점이 나중에야 밝혀졌으나 루머를 해소하는 데 크게 도움이 되진 못했다.[3)4)]

3) 국가인권위원장은 성명을 통해 "감염병의 확산 방지와 예방을 위해 감염환자가 거쳐 간 방문 장소와 시간 등을 일정부분 공개할 필요성 자체는 부인하기는 어렵습니다."라 하여, 프라이버시에 대한 정보주체의 권리가 공공의 이익 등 다른 사회적 가치와 비교형량하여 평가되어야 하는 상대적 가치라는 점에 대해서는 원칙적으로 동의하는 입장을 가지고 있는 것으로 평가된다. 성명의 세부 내용은 다음 링크를 참조할 수 있다. 국가인권위원회, "코로나19 확진자의 과도한 사생활 공개 관련 국가인권위원장 성명", 2020. 3. 9. https://www.humanrights.go.kr/site/program/board/basicboard/ view?board₩-ty-peid=24&boardid=7605121&menuid=001004002001 (최종방문일 2020. 9. 10.)

4) 동아일보, "같은 시간 같은 숙소 머물렀다고… 어느 날 불륜커플이 됐다", 2020. 8. 29. https://www.donga.com/news/article/all/20200829/102697137/1 (최종방문일 2020. 9. 10.)

감염병 환자의 이동경로는 「감염병의 예방 및 관리에 관한 법률」(법률 제16725호, 2019. 12. 3., 일부개정. 이하, '감염병예방법') 제34조의2(감염병위기 시 정보공개) 제1항에 따라 「재난 및 안전관리 기본법」 제38조 제2항에 따른 주의 이상의 위기경보가 발령되는 경우 보건복지부장관이 공개를 하도록 규정되어 있었다. 감염병 환자의 이동경로, 이동수단, 진료의료기관 및 접촉자 현황 등 '국민들이 감염병 예방을 위하여 알아야 하는 정보'를 정보통신망 게재 또는 보도자료 배포 등의 방법으로 신속히 공개하도록 되어 있다. 이동경로 공개와 관련한 범위는 감염병예방법 시행령 제27조의4(감염병위기 시 정보공개 범위 및 절차 등)에 규정되어 있는데, "질병관리본부장은 법 제34조의2 제1항에 따라 정보를 공개하는 경우에는 감염병 위기상황, 감염병의 특성 및 역학적 필요성을 고려하여 공개하는 정보의 범위를 결정해야 한다."와 같이 매우 포괄적인데다 질병관리본부장에 의한 자의적 판단의 여지를 두는 방식으로 규정되어 있다.

질병관리본부는 상기와 같은 규정 방식에 대한 비판이 이어지자, 국가인권위원회의 권고를 반영하여 2020년 3월 14일 <확진환자 이동경로 공개 정책 개선방안>을 마련하였으나, 이 역시 '개인을 특정하는 정보를 공개하지 않음'과 같이 매우 포괄적인 내용으로 구성되어 실효성을 의심케 하였다. 2020년 7월 2일에는 질병관리본부가 코로나19 브리핑을 통해 "성별·연령·국적·거주지(직장명) 등 확진자를 특정할 개인정보 공개를 하지 않겠다."라고 밝혔으나, 이미 이동경로 공개 및 그 과정에서 신상정보 노출에 따른 피해가 적지않게 확인된 점에 비추어 상당히 늦은 조치로 평가받기도 하였다. 질병관리본부가 지난 2019년 11월에 공개한 <공중보건 위험소통 표준운영절차(SOP) 제2판>에서도 이동경로 공개와 관련한 세부적 지침이 부재한 점에 대한 지적이 제기되기도 했다.[5)]

감염병예방법에 의하는 경우 감염병 환자의 이동경로는 보건복지부장관이 수행하는 것이 원칙이었다. 이러한 이동경로 공개 의무는 정부조직 개편에 따라 질병관리청장에게 이관되었고, 추후 개정 감염병예방법(법률 제17475호, 2020. 8. 12., 일부개정)에 따라

5) 졸고, "감염병예방법의 정보공개 규정 살펴보기 - 공공의 건강 및 안전, 그리고 프라이버시의 균형", KISA REPORT 2020 vol.3 (2020. 3. 31.) 참조.

시·도지사 및 시장·군수·구청장에도 경로 공개 의무가 부여되었다.

법 개정 전에도 감염병 환자의 이동경로를 지방자치단체들이 재공개하는 관행은 당연하게 받아들여졌는데, 이것이 언론이나 소셜 미디어 등을 통해 확산되는 과정에서 정보주체를 특정할 수 있는 정보나, 사생활을 침해할 수 있는 정보가 추가되어 확산됨에 따라 심각한 프라이버시 문제를 야기했다. 이와 같은 문제점을 개선하기 위해선 감염병예방법 시행령에 이동경로 공개와 관련하여 ▲동선공개 주체 ▲공개 정보의 범주 ▲동선 정보의 공개기간 및 삭제주기 ▲동선정보 재가공 제한 ▲동선 공개 예외사유 등을 구체화할 필요가 있다고 여러 전문가들이 지적하기도 하였다. 또한 공중보건 위험소통 표준운영절차(SOP)의 개정 내지 별도의 <이동경로 공개 표준운영절차(SOP)>를 마련하여 소위 '프라이버시 보존 정보공개(privacy-preserving disclosure)'의 구체적 방식을 제시할 필요가 있다는 의견이 제시되기도 했다.

이동경로 공개로 인해 공개된 사항이 사실과 다른 경우, 또는 공개된 사항에 관하여 의견이 있는 경우 보건복지부장관에게 서면, 구두, 또는 정보통신망을 통하여 이의신청을 할 수 있고(동법 제34조의2 제2항), 보건복지부장관은 이와 같은 이의가 상당한 이유가 있다고 인정하는 경우에는 공개된 정보의 정정 등 필요한 조치를 하여야 한다(같은 조 제3항). 아울러, 이에 따른 이의신청을 하려는 사람은 동법 시행령 규정에 따라 정해진 서식의 '정보공개 이의신청서'를 질병관리본부장에게 제출하여야 한다(동 시행령 제27조의4 제2항).
그런데, 일견 별 다른 문제점이 없는 것처럼 보이는 이와 같은 이의신청 방식은 다음의 지점에서 생각지 못했던 이슈를 야기할 수 있을 것으로 생각된다. 첫째, 정보공개 이의신청서에는 성명(법인이나 단체의 경우에는 법인이나 단체명 및 대표자 성명을 기재), 생년월일, 전화번호, 팩스번호, 전자우편주소, 정보공개 당사자와의 관계, 주소 및 이의신청 내용을 기재하도록 되어 있어 익명으로는 신청을 할 수 없는 구조다. 이로 인해, '가명 처리된 수준'에서 이동경로 공개가 되었음에도 불구하고, 이에 대한 이의신청으로 인해 그 피해자의 신원이 특정(공개)된다는 문제가 있다. 아울러, 공개된 사항이 사실과 다른 경우에 해당하지 않지만, 공개된 사항에 관하여 의견이 있는 경우라 할지라도 이의신청자의 신

원을 공개해야 하는 부담으로 인해 의견 개진에 나서는 것을 꺼릴 수밖에 없다. 둘째, 공개된 정보에 대한 이의신청을 하는 경우에도 보건복지부장관이 "이의가 상당한 이유가 있다."라고 인정해야 공개된 정보의 정정 등 필요한 조치가 취해지기 때문에, 정보공개로 인해 발생한 피해를 정보주체 등이 직접 입증해야 하는 문제가 있다. 또한, 이의가 '상당한 이유'가 있어야 한다고 규정하는 것은 통상의 이유보다 높은 '고도의 이의 제기 사유'가 존재해야 하는 것이기 때문에 정보주체의 이의가 통상적 수준에서 합리적이라 할지라도 이를 보건복지부장관이 받아들여 공개된 정보의 정정 등 필요한 조치에 선뜻 나서기 어려울 수밖에 없다. 즉 객관적으로 피해가 발생한 것이 명백한 경우가 아닌 다음에야 이의가 받아들여지기 어려운 구조이다. 셋째, 서면 외의 방식으로 이의신청을 하는 경우는 서면에서 요구하는 구체적 신원 정보를 제시하지 않아도 되기 때문에 특정한 이의신청 방식에 의한 신원 특정(공개) 위험이 여타 방식에 비해 높은 구조이다. 구두나 정보통신망으로 이의신청을 하는 경우에 보건복지부장관이 이의신청자의 신원을 확인하는 절차가 내규나 업무지침으로 마련되어 있지 않은 이상, 서면에 의한 이의신청이 정보주체 입장에서 절대적으로 부담스러운 방식일 수밖에 없다. 마지막으로, 이의가 상당한 이유가 있는 것으로 판단된다 할지라도, '공개된 정보의 정정 등 필요한 조치'가 무엇인지에 대해 보건복지부는 구체적 입장을 피력한 바가 없기에, 정보의 정정 외에 기대할 수 있는 조치가 제한적일 수밖에 없다. 통상 'OO 등 필요한 조치'는 'OO에 상당한 조치'를 의미하기 때문에, 공개된 정보의 정정 외에 관계 당국이 소셜미디어에 확산된 정보를 삭제하거나 정보주체에 대한 신원보호 조치를 이행하는 등 보다 '적극적인 조치'에 나설 것을 기대하기는 어렵다고 판단된다.[6)]

6) '상당한'이라는 표현은 통상의 경우와 비교하여 높은 수준의 판단 기준을 요구하는 것으로 이해된다. 이는 영업비밀에 관한 판결에서 자주 확인할 수 있는데, 대법원은 "'상당한 노력에 의하여 비밀로 유지된다.'는 것은 그 정보가 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고, 그 정보에 접근할 수 있는 대상자나 접근 방법을 제한하거나 그 정보에 접근한 자에게 비밀준수의무를 부과하는 등 객관적으로 그 정보가 비밀로 유지관리되고 있다는 사실이 인식 가능한 상태인 것을 말한다."(대법원 2008. 7. 10. 선고 2008도3435 판결)라고 판시하여 '상당한'이라는 표현에 높은 수준의 판단 기준이 요구된다는 점을 객관적으로 제시한 바 있다.

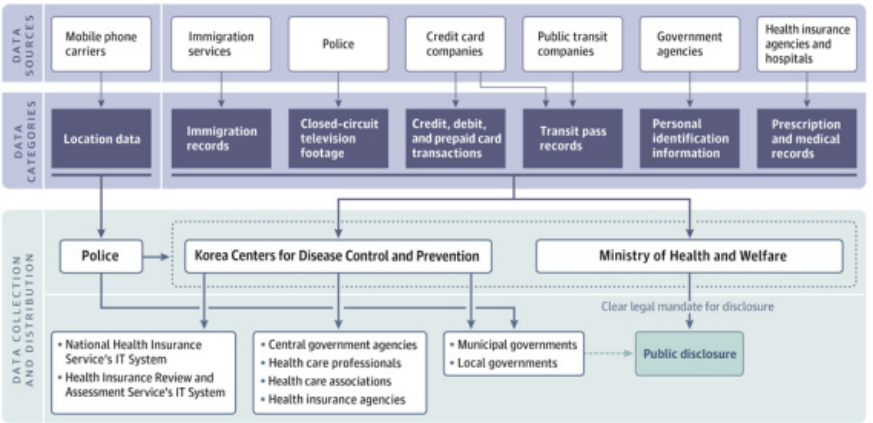
이와 같은 문제점을 해결하기 위해서는 ▲서면과 기타 방식에 의한 이의제기 시, 이의를 제기하는 사람에 관하여 수집하는 정보에 차별이 없도록 규정을 구체화하고, ▲누구라도 익명에 의한 이의제기를 쉽게 할 수 있는 체계(예: 익명 신고 웹사이트)를 구축하는 동시에, ▲보건복지부장관이 수행해야 하는 '필요한 조치'를 구체화하거나, '이의가 합리적 이유가 있는 경우,' 이의 제기된 사안에 필요한 '비례적 조치(proportionate measure)'를 이행하도록 하여 실제 발생한 피해에 상응하는 조치가 진행될 수 있도록 법제를 개선할 필요가 있을 것이다.

3. 감염병 환자 접촉자 추적과 프라이버시 침해

코로나19로 인해 또 다른 프라이버시 논쟁이 발생하고 있는 영역은 감염병 환자와의 접촉을 확인하여 코로나19 감염 의심자를 추적 및 검사하는 소위 '3T' 영역이다. 그 가운데에서도 '감염병 환자 접촉자 추적앱(contact-tracing app)'이 가장 큰 논쟁의 대상이 되고 있다. 우리나라는 일반 대중을 대상으로 한 감염병 환자 접촉자 추적앱을 운용하지는 않지만, <코로나19 역학조사 지원시스템>을 통해 감염병예방법 제76조의2 제1항에 따라 수집할 수 있는 다양한 정보를 자동화된 시스템을 통해 수집·활용한다. 또한, 지난 6월부터는 QR코드에 기반한 '전자출입명부(KI-Pass 시스템)'를 도입해서 사용하고 있다.

[그림-5] 코로나19 역학조사 지원시스템 (출처 : 과학기술정보통신부)

이와 같은 시스템을 구축할 수 있게 된 법적 근거로는 감염병예방법 제76조(정보 제공 요청 및 정보 확인 등)가 있다. 이에 의하는 경우 보건복지부장관 또는 질병관리본부장은 감염병 예방 및 전파의 차단을 위해 필요한 경우, 행정기관, 지방자치단체, 공공기관, 의료기관 및 약국, 법인·단체·개인에 대하여 성명, 주민등록번호, 주소, 전화번호, 진료기록부, 출입국관리기록, 신용카드 사용명세, 교통카드 사용명세, 영상정보처리기기로 수집된 영상정보 등 매우 다양한 정보의 제공을 요청할 수 있으며, 요청을 받은 자는 이에 따라야 한다. 전 세계 그 어느 곳에서도 이와 같이 광범위한 데이터 소스로부터 코로나19 감염 의심자를 추적하기 위한 시스템을 갖추고 있는 곳을 찾아보는 것은 매우 어려운 것으로 알려져 있다.



[그림-6] 감염병 정보 수집 체계 (출처: JAMA)

<코로나19 역학조사 지원시스템>은 감염병예방법의 근거에 따라 구축된 시스템이지만, 이를 통해 수집 등 처리되는 다양한 개인정보에 대한 기술적, 관리적, 물리적 보호조치가 어떻게 구현되었는지 구체적으로 알려진 바가 없다. 정부는 지난 4월 10일 온라인 언론 설명회를 통해 해외 주요 미디어를 포함하는 다수 언론사를 대상으로 설명회를 개최하였으나, 개인정보 처리과정에서의 보호조치에 대해선 ▲2중 로그인 체계 적용 ▲역학조사관만 정보요청 가능 ▲정보제공의 관계기관 승인절차 구현 ▲한시적 정보 활용 등을 밝혔을 뿐, 구체적인 개인정보 보호조치가 어느 정도의 수준으로 적용된 것인지는 밝히지 않았다.[7)]

근래에는 우리나라가 운영하는 '자가격리앱'에서 자가 격리중인 사람들의 신상정보가 노출될 수 있는 취약점이 있다는 사실을 뉴욕타임스(Tne New York Times)가 보도한 바 있다. 구체적으로 ▲ID할당 시 단순한 알고리즘 사용, ▲전송구간 HTTPS 미적용, ▲격

7) 정부24, "「코로나19 역학조사 지원시스템」 온라인 언론 설명회 개최", 2020. 4. 10. https://www.gov.kr/portal/ntnadmNews/2139675 (최종방문일 2020. 9. 10.)

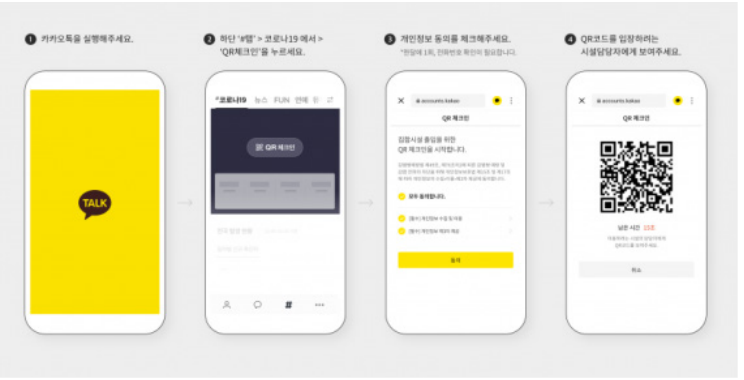
리해제 후 개인정보 수동삭제 등의 문제점이 확인된 것인데, 이를 발견한 서울에 사는 엔지니어인 프레데릭 렉텐슈타인은 해당 취약점을 행정안전부에 제보했으나 미온적 반응을 경험했다고 한다. 행정안전부는 바이러스 확산을 늦추기 위해 가급적 빨리 앱을 배포하느라 서두르는 과정에서 보안성 검토를 하지 못했다며, 최신 버전에서는 지적받은 문제를 해결했다고 설명하였다. 투명하지 못한 감시체계 운영과 당연하게 수행해야 할 절차를 누락하여 발생하는 피해는 고스란히 감염병 환자 및 격리대상자들에게 옮겨졌다.[8)]

이러한 지점에서 노르웨이는 우리나라와 확연히 비교되는 사례를 보여준다. 노르웨이 보건 당국(Folkehelseinstituttet)은 노르웨이 개인정보보호 감독기구(Datatilsynet)의 경고에 따라 2020년 4월부터 배포하여 운영했던 코로나19 감염자 추적 앱 'Smittestopp("infection stop"을 의미함)'의 배포 및 정보 수집을 중단한다 밝혔다. 개인정보보호 감독기구는 노르웨이에서의 코로나19 확산이 제한적이며, 이를 사용하는 인구가 많지 않은 것 등에 기인하는 제한적 효과성을 고려할 때, Smittestopp의 사용으로 인해 발생하는 프라이버시 침해가 앱의 사용으로 인해 얻을 수 있는 효용에 "비례적이지 않다(disproportionate)"는 점을 지적했다. 노르웨이의 인구는 540만 명인데, 앱은 약 60만 명(16세 이상 인구의 약 14%)에 그쳤으며, 6월 2주차까지의 코로나19로 인한 사망자는 242명으로 비교적 제한적이란 점을 고려한 조치이다. 보건 당국은 이와 같은 개인정보보호 감독기구의 평가에 동의하지 않지만, 전달받은 통지의 요구사항에 따라 앱의 추가 배포 및 데이터 수집을 일시 중단한다 밝혔다. 개인정보보호 감독기구는 "보건 당국이 사용한 기술과 앱이 팬데믹 대응에 사용될 수 없다는 것을 의미하지 않지만, 해당 앱의 적법성은 '적용된 조치의 사회적 이익'에 기반해야 한다."라는 입장을 밝혔다. 개인정보보호 감독 기구는 대응의 비례성 외에, 1) 감염 확인과 분석·연구 목적 등 다른 목적에 대한 개별 동의를 수행할 수 없는 점, 2) 블루투스(Bluetooth) 기반이 아니라, 실시간 GPS 위치추적 기반기술을 사용하는 점, 3) 분석 데이터에 대한 익명화 및 총계화 조치가 적절히 적용되지 않은

8) The New York Times, "Major security flaws found in South Korea quarantine app", July 21, 2020, URL: https://www.nytimes.com/2020/07/21/technology/korea-coronavirus-app-security.html

점 등의 구체적 문제점을 지적하기도 하였다. 노르웨이의 사례는 보건당국과 개인정보보호 감독기구의 상호작용을 통한 견제와 균형이 제대로 동작할 수 있음을 보여주는 사례라 할 수 있다.[9)10)]

감염병 환자 접촉자 추적앱은 아니지만, QR코드 기반의 전자출입명부 운영에 대해서도 상당히 많은 관심이 모아졌다. 네이버 앱을 시작으로 하여 이동통신3사의 PASS앱, 그리고 마지막에는 국민메신저로 불리는 카카오톡앱에도 전자출입명부 작성에 필요한 QR코드가 탑재되었다. 집합시설 출입자를 기록하여, 감염병 환자 출입이 확인되는 경우 접촉자 추적을 위해 전자출입명부를 운영하는 것인데, 이 과정에서 생성, 수집되는 정보는 각 앱 서비스 제공사업자들과 사회보장정보원이 분산하여 저장한다. 역학조사가 필요한 경우에만 방역당국이 두 주체에 나뉘어져 있는 정보를 합쳐 이용자를 식별하며 정보는 수집 후 4주 경과 시점에 자동으로 폐기된다.[11)]



[그림-7] 카카오톡 QR체크인 이용방식 (출처: 카카오)

9) Folkehelseinstituttet, “FHI stopper all innsamling av data I Smittestopp”, June 15, 2020, https://www.fhi.no/nyheter/2020/fhi-stopper-all-innsamling-av-data-i-smittestopp/ (최종방문일 2020. 9. 10.)

10) Datatilsynet, “Midlertidig stans av appen Smittestopp”, June 12, 2020, https://www. datatil-synet.no/aktuelt/aktuelle-nyheter-2020/midlertidig-stans-av-appen-smittestopp/ (최종방문일 2020. 9. 10.)

11) 블로터, “카카오톡도 QR 체크인 도입”, 2020. 7. 1. http://www.bloter.net/ archives/393277 (최종방문일 2020. 9. 10.)

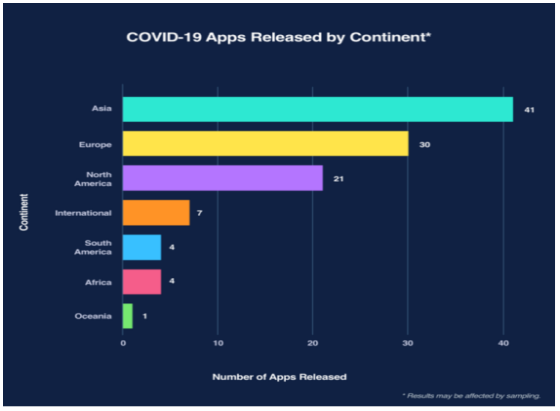
QR체크인 출입명부 도입 과정에서 개인정보영향평가가 진행되었는지 여부는 확인되지 않는다. 이는 상기 <코로나19 역학조사 지원시스템>이나 최근 보안 취약점이 확인된 '자가격리앱'의 경우도 마찬가지다. 「개인정보 보호법」(이하 '개인정보보호법') 제33조 제1항 및 동법 시행령 제35조에 의하는 경우, 아래 4가지 기준에 해당되는 공공기관의 장은 '개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(=개인정보 영향평가)'를 실시하고, 그 결과를 개인정보보호위원회에 제출하여야 한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만 명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조 제1항에 따른 개인정보 영향평가(이하 '영향평가'라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

그러나 개인정보보호법 제33조 제1항에 의한 영향평가는 그 결과를 개인정보보호위원회에 제출하는 것을 의무화하고 있음에도 불구하고, 이를 이행하지 않는다고 하여 처벌 등 불이익을 주지는 않기 때문에 '실효적 강제성'이 없는 것으로 평가된다. 또한 동법 제33조 제3항은 "보호위원회는 제1항에 따라 제출받은 영향평가 결과에 대하여 의견을 제시할 수 있다."라고 규정하고 있을 뿐, 영향평가를 실시하지 않는 경우 이를 이행하도록 강제할 수 있는 규정을 두지 않아 개인정보보호위원회에 의한 영향평가 검토 체계가 무력화될 수밖에 없는 구조적 문제점을 가지고 있다. 또한 개인정보 영향평가 결과의 공개에 관한 사항이 명문화되어 있지 않아, 투명성 확보 및 그에 따른 시민사회 등의 감시도 가능

하지 않은 점은 개인정보보호법의 맹점이라 하지 않을 수 없다.

접촉자 추적 앱에 의한 프라이버시 침해 우려는 개인정보 처리에 대한 투명성(transparency)을 확보하여 일부 상쇄할 수 있다. 국제 디지털 책임성 위원회(International Digital Accountability Council)는 2020년 6월 총 41개국, 108개의 코로나19 관련 모바일 앱을 분석하여 그 결과를 공개하였다. 위원회는 투명성 측면에서 유럽연합 7개, 인도 5개 앱의 개인정보 보호정책(Privacy Policy)을 분석했는데, 유럽연합 앱의 평균 단어 사용이 인도 앱보다 약 2배 가량 많았던 점(약 2,100개 단어 vs. 1,000개 단어) 외에도 유럽연합의 앱이 1) 데이터 수집 방식, 2) 개인정보보호 책임자의 연락처 제공, 3) 데이터 보유 정책, 4) 개인정보에 대한 프라이버시 권리 안내 등에 있어 보다 자세한 설명을 제공하고 있는 점이 확인되었다. 이와 같은 결과는 개인정보 처리 투명성에 있어 어떠한 프레임워크를 보유하고 있는지(유럽연합은 GDPR을 제정)가 의미있는 결과를 보여준다는 시사점이 있다.[12)]



[그림-8] 대륙별 코로나19 관련 모바일 어플리케이션 출시 비교 (출처: IDAC)]

12) International Digital Accountability Council, “Privacy in the Age of COVID: An IDAC Investigation of COVID-19 Apps”, June 5, 2020, p. 6-7, https://digitalwatchdog.org/wp-content/uploads/2020/06/IDAC-COVID19-Mobile-Apps-Investigation.pdf (최종방문일 2020. 9. 10.)

아울러 세계경제포럼(World Economic Forum)은 프라이버시 강화 기술(Privacy Enhancing Technologies)이 코로나19 위기상황에서 프라이버시가 강화된 정보 공유를 가능하게 하여 공공의 보건과 프라이버시의 균형을 이루는 데 도움이 될 수 있다는 견해를 적극 제시하였다. 특히, 감염자 추적 및 검사에 있어 "centralized vs. decentralized 해법"이 존재하는 상황을 인식하면서, 전자는 임계점(critical mass)에 도달할 수 있는 다운로드 확보의 어려움과 보건 당국이 인구 수준에서의 인사이트를 획득하기 어려운 점, 후자는 보건 당국이 요구하는 수준의 스케일과 데이터 상세를 '적절한 수준에서 총계화'할 수 있는지와 보건 당국이 필요로 하는 데이터에 대해 프라이버시가 강화된 방식으로 접근을 허용할 수 있을지의 문제가 있다는 지적을 제기하였다. 우리나라도 법제도 및 방역 시스템 구축에 있어 참고할 수 있는 지점으로 사료된다.[13)]

4. 나가며

코로나19라는 팬데믹에 대응하는 과정에서 '개인정보자기결정권'이라는 우리 헌법상의 기본권에 가해지는 일정 수준의 제한과 관련하여, "우리나라는 2015년도 메르스(MERS, 중동호흡기증후군)를 경험하면서 감염병 대응에 대해 현재와 같은 광범위한 대응 체계를 갖추는 것에 사회적 합의(social consensus)가 이루어진 것으로 볼 수 있으므로 문제가 없다."라고 주장하는 사람들이 적지 않다. 즉, 감염병예방법상의 이동경로 공개, 광범위한 다층적 정보 수집체계 수립 등에 대해 사회적 합의가 있었던 것으로 추정할 수 있기 때문에 프라이버시에 대한 침해를 사회나 개인이 일정 부분 용인해야 한다는 주장이 일부 받아들여지고 있는 것이다.

그러나 이와 같은 사회적 합의의 존재에 대한 주장은 합의의 성립요건을 제대로 제시하지 못하고 있다. 즉 합의가 성립하기 위해서는 의사표시의 객관적 합치와 주관적 합치가 있어야 함에도 "어떤 주체의 의사표시를 확인한 것이며, 그러한 의사표시가 어떤 지점에

13) World Economic Forum, "How privacy enhancing technologies can help COVID-19 tracing efforts", May 22, 2020, https://www.weforum.org/agenda/2020/05/how-privacy-enhancing-technologies-can-help-covid-19-tracing-efforts/ (최종방문일 2020. 9. 10.)

서 합치된 것이며, 이의 객관적 합치를 입증하는 징표는 무엇인가"에 대한 답을 주지는 못하고 있다. 일부에서는 감염병예방법의 제정이 사회구성원 개개의 의사에 대한 객관적 합치라 주장할 수 있을 것이나, 이는 입법 과정이 사회 구성원의 모든 의사를 합치시키는 것이라는 자칫 전체주의적 발상을 정당화할 수 있는 것으로 사회에 사상적 고립의 위기를 야기할 수도 있다. 따라서, 현재의 코로나19 상황에서 정보주체가 갖는 헌법상의 권리인 개인정보자기결정권의 제약에 있어 사회적 합의가 존재한다는 주장을 당연시하는 사회적 분위기는 재고되어야 한다.

이는 개인정보자기결정권이 다른 헌법상의 기본권에 비해 월등하게 우월한 지위를 점하고 있다는 주장을 하고자 하는 것은 아니다. 그러나 개인정보자기결정권이 현재와 같은 기술적 감시 체계에서 초기 프라이버시권이 점했던 '혼자 있을 권리, 물리적 공간에 대한 침해로부터 자유로울 권리' 등에 한정되는 것으로 보는 시각 또한 적절하지 않다. 개인정보자기결정권이 헌법상의 여러 기본권과 비교하여 어떠한 지위를 점하고 있는지 사회적으로 신중한 탐구를 거쳐, 다른 기본권과의 적절한 비교형량을 통해 그 지위에 대한 재평가가 이루어져야 할 것이다. "개인정보자기결정권은 절대적인 권리는 아니고 비례원칙과 명확성의 원칙 등 기본권 제한의 일반 원칙에 따라 제한 가능하고, 다른 기본권과의 충돌이 발생하는 경우에도, 적어도 표현의 자유와는 우열을 가릴 수 없는 권리로서, 기본권 충돌의 일반 법리의 적용을 받는다."라는 한 법률가의 지적을 다시금 새겨볼 때이다.[14)]

미국 시민권리 단체인 뉴아메리카(New America)는 데이터 처리 관행이 사회적으로 내몰린 계층(marginalized communities)을 대상으로 한 감시를 증대시킬 수 있음을 신랄하게 꼬집었다. 또한 개인정보의 부적절한 활용(exploitation)이 사회경제적 불공정을 영속화할 수 있다는 문제점도 지적하였다. 특히, 역사적으로 차별에 노출되어온 특정 계층을 대상으로 한 사회경제적 폐해로 이어질 수 있다는 점을 강조하였다. "가난한 사람들은 양 극단을 경험하는데, 지나친 노출과 비노출(hypervisibility and invisibility)이 바로 그

14) 채성희, "개인정보자기결정권과 잊혀진 헌법재판소 결정들을 위한 변명", 정보법학 제20권 제3호, 한국정보법학회, 2016, 291-328면.

것이다."라는 Valentin의 지적은 현재의 코로나19 상황에도 큰 울림을 준다. 사회적으로 보다 도움이 필요한 사람들에게 프라이버시 이슈는 프라이버시에 대한 권리 침해에 한정되지 않는다는 것이다. 그들은 사회경제적으로 다양한 영역에서 더욱 더 구석으로 내몰리게 된다. 결국 비노출의 지점까지 내몰릴 수 있는 것이다. 이는 프라이버시에 대한 권리가 적절히 보장되지 않는 것에서 시작하는 불평등의 심화라는 결과를 야기한다는 뼈아픈 지적인 것이다. 프라이버시 침해로 인해 촉발되는 다양한 사회경제적 이슈에 대한 법제도적 접근은 그래서 더욱 중요하다.

03 중국 온라인 플랫폼에서의 개인정보 법제 및 실태 분석

지동메이(季冬梅) 교수 (중국 수도경제무역대학교) **백지연** 연구원 (한국법제연구원)

1. 중국 내 프라이버시에 대한 인식의 제고(提高)

중국의 2013년 "주엽(朱烨) v. 바이두" 사건은 대중의 개인정보에 대한 인식의 변화를 가져온 대표적인 사건이다. 원고 주 모씨는 웹사이트를 서핑하던 중 바이두(Baidu) 검색창을 통해 키워드 검색을 한 후, 바이두 온라인 네트워크 연맹(百度网络联盟)에 속하는 특정 사이트에서 자신이 검색했던 키워드와 관련된 광고가 지속적으로 표시되는 것을 발견했다. 원고의 주장에 따르면, 피고 바이두는 이용자의 인지와 선택의 과정없이 네트워크상 기록을 통해 사이트 이용자가 검색한 키워드를 추적하고, 이용자의 관심사나 기호, 생활, 학습, 업무와 관련된 정보를 바탕으로 키워드 검색 기록과 관련된 광고를 삽입하여 원고의 프라이버시를 침해하였다는 것이다. 본 사건의 1심 법원은 피고가 쿠키(HTTP Cookie)기술로 원고의 프라이버시에 해당하는 정보를 무단으로 수집하고, 또 원고가 이를 인지하지 못했으며 나아가 원치 않는 상황에서 상업적으로 이용한 점으로 미루어 보아 피고 바이두가 원고의 프라이버시를 침해하였다고 판단했다. 그러나 2심 법원은 1심과 반대로 개인정보의 '식별 가능성', 개인정보의 사용행위가 인터넷 이용자에게 실질적인 손해를 끼쳤는지 여부와 플랫폼과 이용자 간 협의가 이루어졌는지 여부 등을 사건의 쟁점으로 보아 피고가 쿠키 기술을 이용해 이용자에 맞춤형 추천을 제공한 행위는 프라

이버시에 대한 침해에 해당하지 않는다고 판결하였다.[1)]

중국의 플랫폼 산업은 단기간 안에 급성장하였으며 산업의 초기 성장기 당시 대중은 개인정보를 인격적인 권리, 즉 사생활의 영역 정도로 이해하고 있었으며 빅데이터의 중요성과 그 활용이 대중의 삶을 윤택하게 하기 전까지는 개인정보의 재산적 가치에 대해서는 인식이 전무했다고 볼 수 있다. 중국 정부 역시 국가의 미래 산업으로 촉망받는 플랫폼 산업의 성장을 위해 규제보다는 방임을 선택하는 것이 현실이었다. 해당 판결문이 공개된 후 대중들은 자신들의 사적인 정보가 기업들에 의해 무단으로 수집되었고 또한 이렇게 수집된 정보를 영리의 목적으로 활용하였다는 것에 분노했으며 개인정보는 국가가 나서서 보호해야 하는 가장 기본적인 국민의 권익이며 이를 공익의 목적이 아닌 일반 기업의 사리사욕을 채우는 것에 쓰면 안 된다고 목소리를 높이기 시작했다.

이용자의 기본적인 결정권을 고려하지 않는 법원의 판단에 학계에서도 디지털 경제 시대에서 인터넷 이용자와 온라인 플랫폼 운영자 간의 법적 관계를 어떻게 재정립해야 하는지에 대한 논의가 활발해졌으며, 중국의 핵심 미래 산업으로 꼽히는 플랫폼 산업의 건강한 발전을 위하여 플랫폼 운영자의 개인정보 활용 행위를 어디까지 규제해야 하는지, 이 과정에서 이해관계자의 이익을 어떻게 조율해야 하는지에 대한 연구가 활성화되어 2020년 개인정보보호법이 최종적으로 인민대회에 상정되어 심의를 앞두고 있다.

최근 화제가 되고 있는 안면인식 기술과 관련해 2020년 6월 중국 절강성 항저우시 부양구 인민 법원에서 “안면인식 1호 사건(刷脸第一案)” 공개 심리가 열렸다. 본 사건에서 원고 궈빙(郭兵)은 피고인 항저우 야생 동물원이 진출입 보안 시스템을 업그레이드하기 위해 임의적으로 안면인식 시스템을 도입해 미등록자의 입장을 제한하는 행위가 타당하지

1) ‘주엽과 베이징바이두왕쉰과기회사 간의 프라이버시 침해 항소사건(朱烨与北京百度网讯科技公司隐私权纠纷上诉案)’, 강소성남경시중급인민법원 (2014) 영민종자 제5028호 민사판결문 江苏省南京市中级人民法院(2014)宁民终字第5028号民事判决书 참고.

않다고 주장했다.[2] 현재 중국은 안면인식 기술의 강국으로 떠오르고 있으며 공공기관 및 학교 등의 보안 시스템 혹은 안면인식 결제시스템 등 사람들의 실생활에서 실제로 안면인식 기술이 많이 이용되고 있다. 이러한 기술의 상용화 과정에서 개인 정보와 프라이버시는 위협에 직면해 있다. 얼굴 특징과 같은 개인의 생체정보는 유출 혹은 불법 제공될 경우 이용자의 신체와 재산상의 안전을 해치기 쉽다. 해당 사건은 정보의 과도한 수집에 대한 대중들의 의구심과 생체정보의 유출 가능성에 대한 우려를 여실히 반영한 사례인 만큼 판결 선고 전부터 학계와 실무계의 관심을 모으고 있다. 이처럼 일반적인 개인정보 이외에도 알고리즘, 안면인식, 클라우드 컴퓨팅 등의 인터넷을 기반으로 한 신기술에서 파생되는 개인정보 침해 문제에 대한 법적 대응책 마련의 필요성도 함께 대두되고 있다.

2. 중국 개인정보보호 관련 입법 현황과 문제

중국법 상 개인정보보호와 관련된 최초의 언급은 1954년 제정된 「중화인민공화국 헌법」 제90조 "중화인민공화국의 공민은 주거를 침해받지 아니하며, 통신의 비밀을 법률로 보호받는다"에서 찾을 수 있다. 그러나 해당 조문은 상당히 모호해 다른 법률의 구체적인 이해와 적용에 있어서 실질적인 의미를 갖지 못한 유명무실한 조문이었다. 당시 중국의 개인정보는 주로 민법상 "인격 프라이버시" 조항에 근거하여 보호를 받았는데, 해당 조항의 개인정보의 의미와 범위에 대한 정의가 불분명해 개인정보와 관련된 권익을 효과적으로 보장받지 못했다. 2009년 중국 「불법행위법(권리침해책임법)」 (이하 '침권책임법')에서 프라이버시의 법적 지위가 명확해졌으며, 프라이버시를 법적 보호를 받는 "민사권익"으로 지정하였다. 하지만 해당 법률상의 프라이버시는 "자연인이 누릴 수 있는, 자기 자신과 공공의 이익, 그리고 단체의 이익과 무관한 개인정보, 사적 활동 및 사유 영역을 지배하는 인격권"에 해당한다고 명시되어 있어 매우 넓은 범위의 개념이다. 사실상 프라이버시를 조문화해 개인정보에 대한 보호를 강조하고 있지만, 이에 대한 구체적인 보호 방

2) 롱웨이츄(龙卫球), "디지털 신형 재산권 건립 및 체계 연구(数据新型财产权构建及其体系研究)", 정법논단(政法论坛), 2017년 제4호 참조.

안이나 침해행위 발생 시 구제방안 등의 실효성 있는 규정은 존재하지 않았다.

약 8년 동안 앞서 언급되었던 "주 모씨와 바이두"건과 유사한 사례가 여럿 화제가 되어 프라이버시 보호를 위한 법적 근거의 필요성이 높아지자 2017년 「민법」 총칙 개정 시 개인정보보호가 명시된 규정이 신설되었다. 하지만 「민법」 총칙 개정안 내의 개인정보는 여전히 포괄적이며 프라이버시 관련 문제가 속출하고 있는 플랫폼 및 전자상거래 분야에서 적용하기에는 한계가 있다.

이러한 공백을 보완하기 위한 전자 상거래 및 인터넷 분야에서의 개인정보보호 관련 주요 법률은 2016년 「인터넷안전법(网络安全法)」과 2019년 「전자상거래법(电子商务法)」이 있다. 이 법률에 따라 전자상거래 플랫폼 운영자는 인터넷 안전과 개인정보보호에 대한 법정 의무를 부담해야 한다.[3] 개인정보는 "전자 또는 기타 방식으로 기록된, 단독으로 혹은 다른 정보와 결합해 식별할 수 있는 자연인의 이름, 출생 연도, 신분증 번호, 개인생물식별정보, 주소, 전화번호 등 자연인 개인 신상에 관한 각종 정보를 포함하되 이에 국한되지 아니한다."라고 규정하고 있다. 이는 「민법」총칙의 내용과 일치하며 두 법 모두 개괄식 정의와 세부 내용을 열거하는 방식으로 개인정보의 요소와 특징을 정의하고 기본적인 분류를 규정하고 있다. 개인정보 수집 및 이용 행위는 반드시 법률과 행정 법규에 부합하여야 하며, "합법, 정당, 필요"의 원칙에 따라야 한다. 또한 반드시 이용자에게 개인정보 수집과 관련된 상황을 명확하게 고지하고 이에 대한 이용자의 동의를 얻어야 한다고 규정하고 있다. 법률상 원칙을 기초로 중국국가인터넷정보판공실(中国国家互联网信息办公室, 이하 '중국왕신판')과 공업·정보화부(工业与信息化部) 등 행정기관은 온라인 플랫폼 상 개인정보보호에 관한 행정규정과 시행세칙을 제정하였는데, 구체적으로는 「아동 온라인 개인정보보호 규정」, 「정보통신과 인터넷 이용자 개인정보보호 규정」 등이 있다. 행정

3) 중국 「전자상거래법」 제5조: "전자 상거래 운영자는 경영 활동에서 응당 자원, 평등, 공평, 신의성실의 원칙을 준수하고, 법률과 상업적 도덕에 따라 시장 경쟁에 공평하게 참여하고, 소비자 권익 보호, 환경 보호, 지식재산권 보호, 인터넷 안전 및 개인정보 보호 등 방면의 의무를 이행하여야 하며, 제품과 서비스 품질에 대한 책임을 져야 하며 정부와 사회의 감독을 받아야 한다."

법규와 규정으로 특정 단체, 기업 그리고 행위에 대한 개인정보보호를 구체적으로 요구하고 있어 직접적인 적용이 가능하다. 서비스 기업에 대한 행정 감독 관리로 개인정보 권익에 손해를 입히는 행위를 효과적으로 억제하고 징벌할 수 있으며, 행정법규나 규정을 위반한 자는 반드시 행정법상 책임을 져야 한다.

이어서 2020년에는 「개인정보보호법」 제정에 앞서 이루어진 「민법」 개정에서 "프라이버시와 개인보호" 관련 총 8개 조문으로 구성된 장이 신설되었다. 신설된 조문 중 가장 눈에 띄는 점은 개인정보의 정의와 범위를 한정한 것이다.[4] 그 외에도 개인정보를 처리할 때 반드시 지켜야 하는 원칙 및 프라이버시 침해행위를 상세히 열거하고 있다. 그 외 「기록보관법(档案法)」, 「우편법(邮政法)」, 「여행법(旅游法)」 등의 법률에서도 국민의 개인정보는 반드시 존중받아야 한다고 명시하였다. 보다 실질적인 보호를 위해 「형법」 9차 개정안에서 "개인정보 침해죄"와 "데이터 보안 및 관리의무 이행을 거절한 죄"를 신설해 그 불법행위의 결과가 타인에게 손해를 입히는 경우 형사처벌까지 이어질 수 있어 보다 엄격한 사법 태도를 보이고 있다.

현재 중국에서의 개인정보보호는 여전히 많은 어려움을 겪고 있다. 즉, 법적 근거가 될 법률 규정은 존재하나 아직 미흡하고 분산된 입법 체계로 혼란을 야기하며, 개인정보를 보호하는 동시에 국가 미래전략산업인 플랫폼 산업의 발전을 고려해야 하는 어려움이 있다.[5] 행정당국의 관리감독 체계에 있어 흔히 "구룡치수(아홉 마리의 용이 바다를 다스린다는 뜻)" 현상이 두드러지는데, 인터넷산업, 정보통신, 교육, 의료 등 각 분야 기관의 개입이 발생해 관리 주체와 권한의 범위가 명확하지 않거나, 집행을 서로 미루는 등의 효율

4) 「민법」 제1034조는 "개인정보는 전자 또는 기타 방식으로 기록된 단독으로 혹은 기타 정보와 결합해 식별할 수 있는 자연인의 이름, 출생연도, 신분증 번호, 생물식별정보, 주소, 전화번호, 전자 이메일, 건강정보, 행방 정보 등 특정 자연인의 각종 정보이다"라고 규정하고 있다.

5) 천커(陈科), "파편화에서 시스템화로 향하는 과도기: 2018년 중국 개인정보 안전 보호 발전 보고서(碎片化向系统化的过渡：2018年中国个人信息安全保护发展报告)", 「인터넷과 국가 통치 보고서(互联网与国家治理蓝皮书)」, 2018년, 69~70면 참조.

성 저하에 관한 문제가 꾸준히 제기되고 있다.[6] 이러한 법률 체계상의 문제점을 해결하기 위한 입법적인 노력으로 2020년 7월 「개인정보보호법」 초안이 상정되었으며 중국 정부가 법 통과에 대한 강한 의지를 보이고 있다.

3. 온라인 플랫폼의 개인정보 보호의무 이행을 위한 자율규제

국가차원의 입법적 노력과는 별개로 산업계에서도 국제적인 흐름에 발맞추어 자율규제에 대한 인식이 재고되고 있다. 산업계에서도 별도의 지침을 마련하여 기업 차원의 프라이버시 및 개인정보보호에 대한 사회적 책임을 강화하고 있다. 예를 들어, 중국광고협회 인터넷지부는 2014년 제정된 「중국 인터넷 타겟팅광고 집행을 위한 이용자 정보보호 업계 표준」에서 "온라인 타겟 광고" 행위와 프라이버시 원칙에 대해 규정하고 있다. 이용자와 개인정보 수집, 이용, 공유 및 보호에 대한 협의를 통해 허가를 받고 있다. 결론적으로 중국 온라인 플랫폼에서의 개인정보보호는 "법적 규제-자율규제-상호협의"의 형식으로 구체적인 내용을 지속적으로 개선해 나가고 있다.

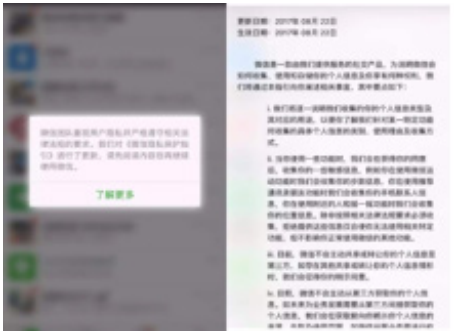
실제로 상호협의 단계의 핵심인 "이용자 협의(개인정보 처리 동의서)"는 인터넷 이용자가 자신의 개인정보 상태를 인지하고 통제할 수 있는 가장 직접적인 방식으로, 최근 중국의 많은 인터넷 기업들도 개인정보 보호의무 차원으로 꾸준하게 진행 중에 있다. 예를 들면 바이두, 위챗, 웨이보 등 웹사이트와 모바일 앱에서 기술을 이용해 타겟팅 서비스를 제공할 때 반드시 이용자와 프라이버시 협의를 체결하여 이용자의 개인정보에 대한 수집, 저장, 공유 여부를 고지하고, 처리 대상 정보 및 서비스 제공자가 이용자 정보 보호를 위해 취하는 조치 등을 설명해야 한다. 온라인 플랫폼 운영자(Internet Service Provider, 이

6) 왕성쥔(王胜俊), "중국 인민대표대회 상무위원회 집행감찰부의 「중화인민공화국 인터넷 안전법」「전국 인민대표대회 상무위원회의 인터넷 정보 보호 강화를 위한 결정」 실시현황 검사 보고(中国"全国人民代表大络会常务委员会执法检查组关于检查《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网信息保护的决定》实施情况的报告)", 전국인대망(全国人大网), 2017. 12. 24. http://www.npc.gov.cn/zgrdw/npc/zfjc/zfjcelys/2017-12/24/content_2036037.htm (최종방문일 2020. 7. 28.)

하 “ISP”) 중 3대 플랫폼 기업인 “BAT(Baidu, Alibaba, Tencent)” 등 기업은 이용자 개인정보 보호를 위해 꾸준히 노력하고 있다.[7] 중국에서 개인정보보호는 과거에는 거의 “공백”과도 다름없었던 상태에서 점차적으로 개선을 거듭해 왔다.

(1) “인지-동의” 원칙과 고지 의무

“인지-동의” 원칙은 개인정보 프라이버시 보호 시 보편적으로 적용되는 원칙이자 정보권자가 자신의 개인정보에 대한 지배권을 행사할 수 있는 구체적인 방법이다. 인터넷 정보 서비스 제공자는 이용자의 동의를 거쳐 개인정보를 수집하고, 반드시 이용자에게 본인의 개인정보 수집과 처리 방식, 내용, 용도에 대해 명확하게 고지하여야 한다. 서비스 제공에 필요한 정보 이외의 개인정보는 수집해서는 아니 되며, 제공하는 서비스 외 다른 목적에 활용할 수 없다. [8] 이용자 동의는 당사자가 충분히 상황을 인식한 상태에서 이뤄져야 하며, 온라인 플랫폼은 반드시 개인정보의 사용 방식, 용도, 목적을 고지해 이를 통해 이용자가 평가와 고려를 거쳐 위탁 여부를 결정할 수 있게 해야 한다.



[그림-9] 위챗 개인정보보호 가이드

7) 바이두가 “바이두 프라이버시 보호 플랫폼”을 설립한 예가 있다. http://privacy.baidu.com (최종방문일 2020. 6. 29.)

8) 「중화인민공화국공업및정보화부령(中华人民共和国工业和信息化部令)」 제20호, 「인터넷 정보 서비스 시장 질서 규범을 위한 약간 규정(规范互联网信息服务市场秩序若干规定)」 제11조.

특히 중국의 대표적인 인터넷 플랫폼 기업인 텐센트는 전문적인 프라이버시 보호 플랫폼을 구축하여[9], 이를 통해 자사 플랫폼의 가치관과 프라이버시 정책 및 보호 가이드를 명시했다. 텐센트가 운영하는 서비스인 "위챗" 역시 회원 가입 절차에서 이용자가 자사의 프라이버시 정책을 읽고 동의를 완료해야 위챗 서비스 이용 권한을 부여하고 있다(위 그림). 이용자의 동의는 명시 또는 묵시의 방식으로 이루어질 수 있는데 여기서 명시적 동의(explicit consent)는 "개인정보주체가 서면, 구두의 방식을 통해 직접 서면 또는 전자 형식의 성명을 내거나 주체적으로 동의의 의사를 표시해, 자신의 개인정보에 대한 특정 처리를 위탁하는 행위"를 말한다. 정보주체는 소극적인 부작위를 통해서도 위탁할 수 있다.[10]

정보 수집이 진행될 때 개인정보주체가 피고의 정보 수집 행위에 대한 고지에도 불구하고 해당 구역을 이탈하지 않거나, 온라인 쇼핑몰 핀둬둬(拼多多)가 프라이버시 정책에서 명시한 대로 "이용자가 일단 핀둬둬의 각종 제품 또는 서비스 사용을 시작하게 된다면 이는 이용자가 본 정책을 충분히 이해하고 동의하는 것으로 간주"할 수 있다.[11]

실제 상황에서 개인정보 관련 내용이 너무 광범위하고, 또 온라인 플랫폼이 상대적으로 기술적 우위를 점하고 있어 프라이버시 정책 공개가 이루어지지 않거나, 정책의 내용이 불명확하다는 문제도 발생하고 있다. 2018년 시행된 실태조사 결과, 중국의 일부 모바일 앱은 3번 이상의 수동 조작이 있어야만 관련 프라이버시 보호 정책 내용을 확인할 수 있으며, 그 중 회원 가입과 로그인 절차를 거쳐야 프라이버시 보호 정책을 확인할 수 있는

9) 구체적인 내용은 "텐센트 프라이버시 보호 플랫폼에서 확인할 수 있다. https://prviacy.qq.com/ (최종 방문 2020. 6. 29.)

10) 중국 전국정보안전표준화기술위원회, 「정보안전기술: 개인정보안전규범」 참고. 2020. 3. 6. 발표, 2020. 10. 1. 시행. http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E (최종방문일 2020. 7. 28.)

11) 핀둬둬 "프라이버시 정책"(최종 업데이트 일자: 2020. 7. 24.)

모바일 앱이 다수 존재함을 확인했다.[12] 그리고 온라인 플랫폼이 프라이버시 보호 정책을 웹사이트나 모바일 앱 화면에서 상대적으로 잘 보이지 않는 위치에 두거나, 프라이버시 정책을 단독으로 보여주지 않고 이용자 협의에 포함시켜 이를 한 눈에 찾기 어려운 상황이 종종 발생하고 있다.

또한 부작위가 동의로 인정되면서 발생하는 문제점도 있다. 정보 수집이 진행될 때 개인정보주체가 피고의 정보 수집 행위에 대한 고지에도 불구하고 해당 구역을 이탈하지 않거나, 온라인 쇼핑몰 핀둬둬(拼多多)는 "이용자가 일단 핀둬둬의 각종 제품 또는 서비스 사용을 시작하게 된다면 이는 이용자가 본 정책을 충분히 이해하고 동의하는 것으로 간주할 수 있다"[13]라고 자사의 프라이버시 정책에서 명시하고 있는데, 이는 사실상 이용자에게 동의를 강제하는 것과 마찬가지라고 볼 수 있다. 프라이버시가 추구하는 개인의 정보 자율성과는 상반되는 행위인 것이다.

또한 온라인 플랫폼에서 사용되는 데이터의 수집, 분석, 처리에 관한 기술은 일반 대중이 알 수 없는 비교적 고도한 기술이고 플랫폼 운영 서버 내부에서 진행되기 때문에 일반 이용자는 이를 알기 어렵고, 설령 이를 인지하더라도 이해하기가 어려워 현실에서는 여전히 개인정보보호의 빈틈이 존재한다.

2018년 공업·정보화부 정보통신관리국은 바이두, 알리페이, 바이트댄스 3개 기업이 회원의 개인정보 수집 및 이용 규칙과 이용 목적에 대해 충분히 고지하지 않은 정황을 포착해, 즉각적인 수정을 요구하여 인터넷 이용자의 알 권리와 선택권을 보장하게 하였다. 중

12) 뉴징(牛静), 런이린(任怡林) , "이동 인터넷 시대의 모바일 앱 프라이버시 정책과 사회적 책임에 대한 탐구—50조항 모바일 앱 프라이버시 보호정책 내용에 근거한 분석(移动互联网时代APP的隐私政策与社会责任探讨——基于50款移动APP隐私保护政策内容的分析" , 「뉴미디어사회책임블루북(新媒体社会责任蓝皮书2018)」, 사회과학문헌출판사, 2018년, 190면.

13) 핀둬둬 프라이버시 정책(최종 업데이트: 2020. 7. 24) https://en.pinduoduo.com/ (최종방문일 2020. 7. 29.)

국에서도 이미 각종 입법 조치를 통해 온라인 플랫폼 운영자가 “인지-동의” 원칙을 반드시 준수하며 정책 고지 의무를 이행해야 함을 명시하였지만, 해당 규칙을 구체적으로 어떻게 적용하고 방대한 양의 개인정보 안전과 보호를 어떻게 철저히 실행할지는 여전히 끊임없는 탐색이 필요해 아직 갈 길이 멀다.

(2) 행위유형별 법적 규제 및 문제점

인터넷 플랫폼 운영자가 이용자의 개인정보를 처리하는 행위를 유형화하면 총 4분류, 즉 정보 수집, 저장, 이용 및 공유로 나눌 수 있다.

먼저, 정보의 수집행위는 이용자로부터 개인정보 제공의 동의를 받는 형태로 이루어진다. 이 과정은 “인지-동의” 원칙에 따라 진행되어야 하며 플랫폼 운영자는 정보수집의 용도, 목적, 방식을 고지하여야 한다. 구체적으로는 “필요·최소”의 원칙에 따라 개인정보를 수집해야 하며, 정보의 주체가 위탁을 동의한 목적에 부합하는 범위에 한하여, 최소한의 유형과 수를 처리할 수 있다. 그러나 플랫폼의 실제 운영에서는 동의를 강제하거나, 과도한 권리를 요구하거나, 정해진 범위 외의 개인정보를 수집하는 등의 문제가 빈번하게 발생하고 있다. 이를 단속하기 위해 2019년 중국 왕신판(网信办), 공업·정보화부, 공안부, 시장관리감독총국 4개 기관이 공조해 「모바일 앱(APP)의 개인정보 수집 및 이용 위반행위 인정방법(App违法违规收集使用个人信息行为认定方法)」[14]을 실시하였으며 이에 의거해 집중 단속을 시행하기도 하였다.

“인지-동의”의 과정을 거쳐 수집된 개인정보를 저장하는 경우, 개인정보의 저장시간을 최소화해야 하고 기간이 지난 개인정보를 반드시 적시에 폐기하여 개인정보 유출 또는 기타 손해 발생을 막아야 한다. 왕신판(网信办), 공업·정보화부 등 여러 행정 기관에서 각종 행정규칙을 제정해 인터넷 플랫폼 운영자에 개인정보 안전보장 의무의 이행을 요구함

14) 중국 국가인터넷정보판공실, “개인정보보호의 과학적 처리의 중요 성과, 종합적 처리의 중요한 돌파구(个人信息保护科学治理的重要成果、综合治理的重要突破)” , 2020. 1. 4. http://cac.gov. cn/2020-01/04/c_1579683536339887.htm (최종방문일 2020 7. 29.)

과 동시에 통신보안 리스크 관리를 요구했으나, 아직도 인터넷 플랫폼 운영자의 정보 저장과 관련된 구체적인 책임과 의무, 그리고 데이터 안전기술표준 분야의 통일성, 체계성, 실효성을 갖춘 규정은 없는 상황이다. 이 때문에 최근 중국은 「개인정보보호법」 발의에 이어 「데이터 안전법(数据安全法)」을 제정하고자 노력 중이다. 이 법은 데이터 처리자의 데이터 보안 보호의무 이행을 상세히 규정하여 향후 개인정보를 포함한 데이터 보안 강화를 보장해 줄 것이라는 기대를 모으고 있으나 아직까지 의견 청취 과정에 머물러 있어 실효성을 갖추려면 시일이 더 소요될 것으로 보인다.

개인정보 수집의 최종 목적은 수집된 개인정보를 활용해 최종적으로 정보를 가치로 전환하는 것이다. 대표적인 것이 이용자의 정보를 분석해 맞춤형 서비스를 제공하는 것이다. 「인터넷 정보 서비스 시장 질서 규범을 위한 약간 규정(规范互联网信息服务市场秩序若干规定)」은 인터넷 플랫폼 운영자가 이용자의 정보를 서비스 제공 이외의 목적으로 사용하지 아니하여야 한다고 명시하고 있다. 텐센트 프라이버시 플랫폼도 역시 “사용자 개인정보를 이용하기 전 반드시 구체적인 활용 용도에 대해 설명하고, 만약 새로운 혹은 별도의 활용이 있을 경우 이에 대해 사용자의 재동의를 구하여야 한다.”라고 명시하여 플랫폼의 자율규제 방향도 정부와 비슷한 방향으로 나아가도 있다. [15)]

그럼에도 불구하고 현실에서는 여전히 이를 위반하고 개인정보를 부당하게 이용하는 상황이 발생하고 있다. 특히 금융 관련 온라인 플랫폼은 “특별재난지역”이라고 불릴 정도로 그 상황이 혼란스럽다. 2019년 모바일 앱 “장상생활(掌上生活)”은 이용자의 동의를 거치지 않고, 가명처리를 하지 않은 개인정보를 거투이(Getui, 个推, 데이터 분석기업), 센서스 데이터(Sensors Data, 神策数据, 빅데이터 분석 기업), 웨이보(微博) 등 제3자에게 대가를 받고 제공하여 논란을 야기했다. 2019년 해당 사건으로 인해 금융관련 개인정보가 암암리에 거래되고 있다는 것이 알려졌으며 다른 플랫폼에도 관련 정황이 더 있지만 사

15) 텐센트 프라이버시 보호 플랫폼, 「개인정보보호정책」(2020. 4. 7. 업데이트). https://prviacy.qq.com/ (최종방문일 2020. 7. 29.)

실상 현재의 법률체계에서는 이를 특정해 규제하고 있지 않다.
직접적인 개인정보 분석과 처리 이외에도, 인터넷 플랫폼 운영자는 공유 및 양도의 방식으로 정보의 2차 활용을 통해 데이터를 가치화하고 있다. 중국 「개인정보안전규범(个人信息安全规范)」은 개인정보의 활용을 위임받은 주체가 개인정보를 공유 및 양도할 때 반드시 그 리스크를 충분히 고려할 것을 규정하고 있다. 텐센트 프라이버시 플랫폼은 서약서를 통해 "정보의 공유를 엄격하게 제한하여 이미 공유에 관한 동의를 얻은 정보 외에는 이용자의 정보를 공유할 수 없다"라고 명시하고 있다.

그러나 실생활에서 이용자가 인터넷 플랫폼의 행위를 감시하거나 추적하기는 어렵다. 플랫폼 내부 서버에서 이뤄지는 소스 코드가 공개되지 않는다는 사실과 고도의 정보통신 기술의 사용, 플랫폼이라는 가상공간의 허구성 등 여러 요소가 맞물려 실제로 이용자들이 자신의 개인정보가 처리되는 현황을 알기란 매우 어려운 일이다. 그 예로 알리바바[16] 그룹 산하에는 '타오바오(淘宝, 온라인통신판매)', '알리페이(支付宝, 모바일결제시스템)', '페이주(飞猪, 여행용품판매)', '셴위(闲鱼, 중고거래)', '차이냐오궈궈(菜鸟裹裹, 택배 배송 조회)' 등 셀 수 없는 소규모 플랫폼이 있으며 그 중 커머스 플랫폼인 '타오바오'와 모바일결제시스템 '알리페이' 사이에서 개인정보는 자동적으로 공유되어 온라인 거래를 활성화하고 있다. 중국의 전자결제 시장은 지난해 말 기준 56조 2,000억 위안(9,600조 원) 수준에 이르며 이 중 54%가 '알리페이'를 통한 거래액이다.[17] 최근 중국 현지에서는 현금, 카드 등은 국민들의 지갑에서 자취를 감춘 지 오래이며 모든 거래행위가 다 서비스제공 플랫폼과 연동된 알리페이와 같은 모바일결제시스템으로 이루어지고 있다. 모든 거래행위가 밀접하게 연관이 있어 그룹 산하의 플랫폼들은 이용자들의 개인정보를 서로 공유하고 있다. 하지만 이용자가 플랫폼에 최초로 개인정보를 제공할 시 어떤 제3자에게 해당 정보가 제공되는지에 대해서는 프라이버시 약관 중 명확한 설명이 없는 경우가 대부분이

16) 중국 내 3대 인터넷 플랫폼 기업.

17) 김인경, "中, 정부판 디지털화폐 가동에.. 알리페이 정조준", 이데일리, 2020. 8. 9. https://www.edaily.co.kr/news/read?newsId=01321846625865680&mediaCodeNo=257&OutLnkChk=Y (최종방문일 2020. 9. 11.)

다. 이런 점을 악용하는 플랫폼의 경우 불공정한 조항까지도 포함하고 있다.[18)]

또한, 안면인식과 결제 기능이 결합된 모바일 앱을 이용하면 신체 일부의 특징을 통해 거래가 이뤄져 핸드폰이나 카드 등 매체를 휴대할 필요가 없다.[19)] 관련 설문조사 응답자 중 40.2%가 슈퍼마켓과 편의점에서, 36.8%가 마트에서 안면인식 결제를 이용하는 것으로 나타났다.[20)]

결제뿐만 아니라 안면인식 기술은 보안 시스템 강화에도 보편적으로 이용되는데, 이는 보안을 강화하려는 관리자 측에서 임의적으로 도입하는 경우가 많아 이용자들의 선택권이 전혀 고려되지 않고 있다. 보안을 통과하기 위해서는 본인의 생체정보를 반드시 제공하여야 하며, 추후 그 필요가 없어지는 경우에도 해당 정보가 자동으로 삭제되지 않는다면 개개인이 삭제를 요청해야 하는데, 일반적으로 일회성 안면인식의 경우 개인이 이를 인지하고 삭제를 요청하는 경우는 많지 않다. 안면인식 기술의 데이터 처리자와 개인정보의 주체 사이에 존재하는 심각한 불균형으로 개인은 복잡한 알고리즘 이면에서 일어나는 행위들을 통제할 수 없다는 문제점이 있다.

이와 같은 불균형을 해소하기 위해 중국 정부는 「인공지능 금융 모바일 앱 알고리즘 관련 평가 규범(人工智能金融应用算法评价规范)」, 「안면인식 오프라인 결제 모바일 앱 관련 기술 규범(人脸识别线下支付安全应用技术规范)」 등과 같은 다양한 관련 규범과 표준

18) 마이마이(Maimai, 脉脉) 서비스 제공 동의서 중 "타오유 회사가 제3자 파트너사에 연결된 온라인 서비스를 제공하는 상황에서 만약 제3자가 본 동의서에서 약정한 프라이버시 보호 조항과 동등한 책임을 질 것을 동의할 경우 타오유 회사는 이용자 정보를 제3자에게 제공할 권리가 있고, 이용자의 재동의를 받지 아니하여도 된다."라고 언급하고 있다. 양쉐란(杨雪兰), 리웨이동(李卫东)의 "온라인 소셜미디어 서비스 제공자의 개인정보보호 현황 연구 보고(社交网络服务提供商对个人隐私保护现状研究报告)", 《인터넷과 국가 통치 발전 보고(互联网与国家治理发展报告2018)》 (2018년판) 참조.

19) 위이난(于一男) , "안면인식 결제 모바일 앱 연구(人脸识别支付应用研究)" , 금융종횡(金融纵横), 2019년 참조.

20) 첸잔산업연구원(前瞻产业研究院), "2020-2025년 중국 이동 결제 산업 시장전망 및 투자전략 계획 분석 보고서(2020-2025年中国移动支付行业市场前瞻与投资战略规划分析报告)" 참조.

의 제정을 준비하고 있지만, 이는 중국의 안면인식 기술과 같은 신기술과 온라인 플랫폼의 융합 과정에서 파생되는 다수의 개인정보보호 문제를 해결하기엔 무리가 있다.

4. 결론

아직까지 중국 내 인터넷 플랫폼에게 개인정보란 이용자들이 자신의 서비스를 사용하는 과정에 있어서 하나의 부수적인 것에 그친다. 이렇듯 개인정보의 중요성과 그 진정한 가치를 인식하지 못하고 있기 때문에 개인정보는 단순히 기업들의 마켓팅을 위해 사용되고 있다. 특히, 개인정보 제공 및 활용에 동의하지 않을 시 서비스 이용이 종료되도록 한 조치는 사실상 개인정보의 가치가 무색해지게 하는 부분이다. 현재 중국의 법체계에 개인정보와 관련된 여러 법 규정이 존재하나 대부분 포괄적인 규정이 많아 위와 같이 기업들이 이용자들을 상대로 개인정보 제공 및 활용에 대한 동의를 강제하는 경우 마땅히 대응할 방법이 없는 것이 현실이다. 반면, 한국의 「개인정보 보호법」에는 "개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다."라는 조항이 있다(제16조 제3항). 이와 유사한 조항이 올해 발의된 중국의 「개인정보 보호법」에 신설된다면 플랫폼 이용자들의 개인정보를 조금 더 효과적으로 보호할 수 있을 것이다.

중국의 개인정보와 관련된 법제화는 이제 시작에 불과하다. 개인정보 관련 단독 법률인 「개인정보 보호법」이 상정되었을 뿐 정식으로 시행되기까지 많은 시일이 소요될 것이다. 실제로 개인정보보호의 이면에는 정보주체와 정보처리자 간의 이익 다툼이 존재하고 있어, 한국과 같이 개인정보에 대한 강력한 보호는 온라인 플랫폼 운영자가 더 큰 책임과 비용을 부담하여야 한다는 것을 의미한다. 이는 기술과 산업의 발전에 걸림돌이 될 수 있어 일각에서는 우려가 크다. 하지만 이제는 개인정보가 공공의 이익을 위한 것이 아닌 오로지 영리의 목적을 위해 사용되는 것을 지양해야 한다. 국민의 기본적인 정보 자율권을 인정함과 동시에 데이터를 활용한 공익적 사업을 활성화해 정보의 주체와 이용자 상호간의 균형과 조화를 이뤄야 한다. 중국에서도 인공지능, 안면인식, 빅데이터와 클라우드 컴퓨팅 등 기술의 발전이 가져온 개인정보보호 안전에 대한 위협에 맞서 리스크 관리와 대응

조치에 대한 연구를 지속하고 있다. 한국 역시 이러한 사례를 참고하여 적절한 예방과 관리를 통해 사회 전체 이익의 최대화를 가져올 수 있을 것이다.

2020
사회적가치
ISSUE BRIEF
프라이버시

발행일 2020년 10월 31일

발행인 김계홍

발행처 한국법제연구원

세종특별자치시 국책연구원로 15(반곡동, 한국법제연구원)

www.klri.re.kr

ISBN 979-11-973721-1-7 93360

SOCIAL VALUE ISSUE BRIEF

추천사

빅데이터와 AI 기술을 비롯한 신산업의 성장, 코로나19와 비대면 사회로의 전환은 프라이버시와 개인정보에 관한 헌법적 논의와 중요성을 더없이 부각시키고 있다. 한국법제연구원의 <사회적 가치 이슈브리프 2>는 우리 사회가 포착해야 할 사회적 가치로서의 '프라이버시(privacy)'를 민주주의와 법치주의에 관한 근본적인 고민을 담아 심도 있게 조망하고 있다. 무엇보다 주권자인 우리 모두의 프라이버시와 개인정보, 데이터 등의 쟁점을 놓고 하나의 장(場)에서 소통할 수 있는 계기를 마련하였다는 점에서 뜻깊다.

2020. 10.

서울대학교 제26대 총장 성 낙 인

값 7,000원

93360

9 791197 372117

ISBN 979-11-973721-1-7

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE