서울대학교
인공지능정책
이니셔티브

차분 프라이버시(Differential Privacy)의 가능성과 한계

이슈페이퍼 2020-1

# 데이터 3법 시대의 과제:

- 가명처리
- 연구목적 활용
- 차등적 프라이버시
- 데이터 거래

http://sapi.co.kr/

# 차분 프라이버시(Differential Privacy)의 가능성과 한계

**고학수** 서울대학교 법학전문대학원 교수
**구본효** 서울대학교 법과대학원 박사과정

## 요약문

차분 프라이버시(Differential Privacy)는 충분한 수준의 프라이버시 보호를 제공하는 동시에 데이터 분석이나 컴퓨팅 작업을 통해 유용한 결과를 도출해 낼 수 있는 방법론을 마련하는 데에 있어 유용한 개념으로 주목을 받아왔다. 이 개념은 특히 공학 연구자들의 주목을 받아왔는데 그 이유 중 하나는 프라이버시 보호의 수준에 관해 수학적으로 명확한 기준을 정하여 규정할 수 있다는 점에 있다. 그런데 이러한 방식으로 개인정보의 보호에 관해 규정하는 것은 법규범을 통해 개인정보를 정의하고 그에 관해 규율하는 방식과는 상당히 다른 것이다. 따라서 차분 프라이버시 개념의 적용을 통한 개인정보 보호의 방식과 법규범의 해석과 적용을 통한 개인정보 보호의 방식 사이에 어떤 차이가 있는지에 대해 명확히 파악하고 비교할 필요가 있다. 차분 프라이버시는 법규범상으로는 추상적 판단의 대상으로만 고려되기 쉬운 개인정보 활용으로부터의 효용성과 정보주체의 프라이버시 보호를 통해 달성할 수 있는 가치 사이의 상충관계에 관하여 측정가능한 형태의 개념설정과 이론을 제공한다는 점에서 유용하다. 그러나 프라이버시 예산의 설정을 둘러싼 논란이 발생할 수 있고 또한 이를 구현하는 과정에서 상당한 비용이 소요된다는 현실적인 한계가 존재하기도 한다.



## 1. 서론

충분한 수준의 프라이버시 보호를 제공하는 동시에 데이터 분석이나 컴퓨팅 작업을 통해 유용한 결과를 도출해 낼 수 있는 방법론을 마련하는 것은 오래전부터 연구자들의 관심을 받았다. 1978년에 마련된 미국 상무부 보고서에는 개인정보의 보호가 새로운 문제가 아니고, 다만 컴퓨터의 활용도 증대 그리고 이와 함께 상세한 통계에 대한 요구가 증가하였기 때문에 개인정보보호에 대한 관심 또한 이전보다도 고조된 상황이라는 설명이 나타난다.[01] 이러한 설명에 담겨있는 문제의식은 관련 기술이 크게 발전한 지금도 마찬가지로 유효한 것이다. 개인정보의 보호는 공학과 법학을 포함한 여러 영역의 공동의 과제라 할 수 있다.[02] 특히 최근에 관심이 크게 늘어난 빅데이터 분석이나 인공지능 영역에 있어서는 공학, 통계학, 법학 등 관련 영역의 접근이 서로 보완적인 역할을 하면서 함께 노력을 기울일 필요가 있다. 그러나 이러한 개별 영역의 연구는 각 영역 내에서 개별적, 독립적으로 수행되어온 경우가 많고, 그로 인해 관련 사안에 관해 서로 다르게 이해하기도 하면서 사회적으로 유용한 해법을 제시하는데 한계를 보이기도 하였다.[03] 이 글이 논의할 내용은 프라이버시 보호를 위한 기술적 방법론에 관하여 컴퓨터 공학과 법학 사이의 간극을 좁히기 위한 시도의 일환이다.

통계적인 관점에서 보면, 개인정보의 보호는 개인정보의 처리를 통해 유용한 결과를 얻을 수 있는 가능성과 그 과정에서 정보주체의 프라이버시가 침해될 수 있는 가능성 사이에서의 상충관계(trade-off)를 고려하여 해법을 찾아가는 과정인 것으로 이해할 수 있다. 개인정보의 활용을 통해 얻을 수 있는 사회적, 경제적 의의는 상당한 것이다. 그에 관해 법문에 명시적으로 언급되는 경우도 있다. 예컨대 유럽의 개인정보 보호법인 General Data Protection Regulation ("GDPR")에는, 기록부(registries)로부터의 과학적 연구는 지식에 기반한 정책의 실현과 삶의 질 그리고 사회적 서비스(social service)의 제고를 뒷받침하는 견고한 고급의 지식(solid, high-quality knowledge)을 제공할 것이라는 설명이 나타난다.[04] 데이터 분석의 맥락에서 보면, 개인정보의 이용은 데이터를 이용하여 일정한 계산(computation)을 하고 그로부터 추론(inference)을 하는 과정으로

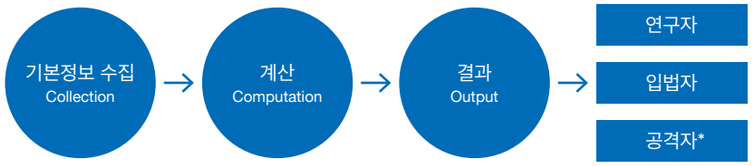
01 Office of Federal Statistical Policy and Standards, "Report on Statistical Disclosure and Disclosure Avoidance Techniques", U.S. Department of Commerce (1978), 1-2.

02 Nissim et al., "Bridging the Gap Between Computer Science and Legal Approaches to Privacy", 31(2) Harv. J.L. & Tech. 687, 730-734 (2018).

03 Kobbi Nissim and Alexandra Wood, "Is Privacy Privacy?", 376(2128) Phil. Trans. R. Soc. A 1, 1-3 (2018).

04 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, Recital (159).

이해할 수 있다[그림1]. 그리고 이로부터 사회적, 경제적 의의를 도출해 내는 과정을 포함할 수도 있다. 연구자나 입법자들이 근거기반의 정책(evidence-based policy)을 만들어 내기 위해서는 데이터를 이용하여 실증적으로 뒷받침하는 것이 가능해야 한다. 다른 한편 제3자(motivated intruder)에게 정보가 제공된 것으로 인해 정보주체의 권리가 침해될 가능성도 존재하므로, 그와 관련된 리스크를 어떻게 최소화 할 것인지에 관한 고려도 물론 중요한다.




[그림 1] 개인정보의 이용 과정[05]

한편, 통계학 또는 공학적 분석과 관련된 맥락에서는 개인정보의 보호에 관해 유사한 개념이 서로 다른 이름으로 불리는 경우도 있어서 유의해야 한다. 예를 들어, 통계학에서는 '통계적 노출 통제(statistical disclosure control; statistical disclosure limitation)'가 종종 중요한 개념으로 등장하는 한편, 컴퓨터 공학에서는 '프라이버시를 보존하는 데이터 공개와 분석(privacy preserving data publishing; privacy preserving data mining)'이 언급된다. 또한 분석이나 이용 맥락에 따른 차이도 존재한다. 예를 들어, 제3자에게 개인정보를 제공하게 될 가능성이 있다면 주로 개인정보에 대한 접근통제 및 데이터 관리가 주요 관심사안이 될 것이고, 개인정보를 변환한 결과를 제공하는 경우라면 이를 이용한 데이터의 분석이 주로 논의될 것이다.[06] 비식별처리(de-identification), 가명처리(pseudonymization), 익명처리(anonymization) 등은 모두 개인정보의 보호에 도움을 주는 데이터 변환 방법론이다. 이러한 방법론의 구체화 과정에서, 컴퓨터 공학이나 통계학 연구자들은 데이터의 '변조(perturbation)'나 '질의의 제한(query set restriction)' 등에 관심을 두고 연구해 왔다.[07] 변조는 주어진 데이터 자체에 대한 변조(data perturbation)와 결과의 변조(output perturbation)로 구분하여 생각할 수 있다. 그리고 질의의 제한은, 데이터 자체에 대한 접근은 허용하지 않으면서 제한된 질의과정을 통해 데이터에 대한 처리와 분석이 가능하도록 하는 방식이다.

이 글이 다루고 있는 차분 프라이버시(differential privacy, "DP")는 개인정보의 보호에 관해 수학적으로 규정한 것이다.[08] 연구자들은 DP로부터 수학적 증명이 가능한 수준의 명확한 프라이버시 보호(formal privacy)가 제공될 수 있다고 주장하였다.[09] 이 개념이 가진 수학적 엄밀성은 이 개념에 대한 통계학이나 컴퓨터 공학 연구자들의 관심을 높이는데 기여하기도 했다. 근래 들어, 2020년부터 미국의 인구조사(Census)에 DP 방법론이 적용될 것이라는 발표가 나온 이후로 DP 개념에 관심을 가지는 연구자들의 범위가 더욱 확대되기도 하였다. 인구조사에 DP 방법론을 도입하는 것에 대해서는 관련 데이터에 담긴 개인정보의 사회적, 경제적 의의의 상실이 우려된다는 비판도 등장하였다.[10] 비판적인 시각의 등장을 포함하여, DP 개념에 대한 연구자들의 관심이 늘어나고 있는 것은 분명한 것으로 보인다.

국내에서는 개인정보 보호법을 포함한 '데이터 3법'이 국회를 통과한 이후로 가명처리 개념이 데이터에 관한 논의의 중심이 되었다. 가명처리는 가장 직접적으로는 식별(identification)의 개념과 연관이 높은 것이다. 식별가능성을 기준으로 개인정보의 개념을 정의하고 있는 법의 규정방식을 고려하면 이는 자연스러운 것이다. 그러나 DP는 그보다 좀 더 근본적인 차원에서, 통계학이나 공학의 시각에서의 프라이버시와 법학의 시각에서의 프라이버시가 양립가능한 것인지(compatibility)에 관해 의문을 제기한다. 한편, 지금까지 DP 개념을 둘러싸고 연구와 논의가 전개됨에 있어 현실적으로는 법학 관점의 시각이 반영되는 데에 한계가 있었던 것으로 보인다. 이는 주로 DP 개념의 수학적 특징에 기인한 것이다. 이 글은 법학자에게도 접근가능한 관련 설명을 제공하여

05 Nissim et al., supra note 2, 695-706.

06 개인정보가 담긴 데이터의 공개는 가능한 결과의 전체를 제공하는 것을 의미할 수 있는데, 그런 경우에 전자의 방식을 통한 프라이버시 보호는 후자의 방식을 통한 보호보다 더 어려울 가능성이 있다. Rakesh Agrawal and Ramakrishnan Srikant, "Privacy-Preserving Data Mining," Proceedings of the 2000 ACM SIGMOD International Conference on Management of data 439, 439-450 (2000).

07 Nabil R. Adam and John C. Worthmann, "Security-Control Methods for Statistical Databases: A Comparative Study", 21(4) ACM Comput. Surv. 515, 516-522 (1989).

08 DP 라는 용어의 유래는, 일반적으로 차분공격이라고 옮기는 "differential cryptanalysis"와 관련이 있는 것으로 보인다. 그렇게 보면, DP의 한글 표현은 "차분 프라이버시"라고 하는 것이 적절할 것이다. 그러나 일반적으로 통용되는 한글 표현이 있는 것은 아니다. 한글로 '차분'이라고 표현하는 경우와 '차등'이라고 표현하는 경우가 모두 발견된다, 구글과 애플은 DP 개념을 "개인정보 차등보호", "차등 개인정보 보호" 등으로 한글화하여 설명하였다.

09 Cynthia Dwork, "Differential Privacy", Automata, Languages and Programming, Springer Berlin Heidelberg (2006), 8-12.

10 Khaled El Emam and Cecilia Alvarez, "A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques", 5(1) International Data Privacy Law 73, 86-87 (2015); Ruggles et al, "Differential Privacy and Census Data: Implications for Social and Economic Research," 109 AEA Papers and Proceedings 403, 403-408 (2019).

향후 논의에 참여할 수 있도록 도움을 제공하고자 한다.[11] 구체적으로 이 글은 다음과 같은 세 가지 질문에 답을 하는 것으로 구성되어 있다. (1) DP는 무엇을 의미하는가? (2) DP는 실현이 가능한 것인가? (3) DP는 어떠한 한계를 가지고 있는가?

11 좀 더 기술적인(technical) 문헌에 관심이 있는 독자들은 각주 및 참고문헌에 제시된 문헌을 참조.



**개인정보보호를 위한 기술적 방법론**

합성데이터(Synthetic data), 동형암호(Homomorphic encryption), 연합학습(Federated learning)

DP와 별도로, 합성데이터, 동형암호, 연합학습 등의 개념도 개인정보를 보호하는 동시에 분석을 가능하게 해주는 방법론으로 근래에 주목을 받고 있다. 이에 관해 간략히 살펴보면, 우선 **합성데이터**는 개인정보의 속성이 고려된 모델을 생성하고 그로부터 가상의 인위적인 데이터를 합성하여 생성하는 방식을 이용하는 것이다. 개인정보가 포함된 데이터셋의 확률분포를 재현한다는 점에서 재현데이터라고도 말한다.[12] 합성데이터는 원칙적으로 정보주체와 체계적인 연결(link)이 가능한 데이터가 아니기 때문에 개인정보로 보기 어렵다. 합성데이터 모형은 개인정보가 가지는 (준)식별정보는 부분적으로 재현하고 속성정보는 대체로 그대로 재현하는 것을 목표로 하여 구축된다. 이런 방식을 통해, 프라이버시를 일정 수준 이상으로 보호하는 동시에 데이터에 담긴 의미가 분석자에게 최대한 제공될 수 있도록 하는 것을 목적으로 한다. **동형암호**는 개인정보를 암호화하고 암호화된 상태에서 그대로 연산을 하여 변환된 결과를 필요에 따라 복호화하는 것으로, 개인정보를 이용한 결과와 암호화된 데이터를 이용한 결과가 동일하도록 하는 체계를 갖도록 하는 방식이다. 동형함호를 이용하면 연산에 앞서 복호화를 하지 않아도 되므로 관련된 프라이버시 리스크가 자연스럽게 최소화될 수 있다. 연산의 속도가 느린 것이 한계인데, 연산 속도를 줄이는 방향의 연구가 지속적으로 이루어지고 있다. **연합학습**은 인공지능 기계학습(machine learning)의 유용성을 높이기 위한 맥락에서 주로 언급되는 보호의 방법으로, 정보주체가 이용하는 기기로부터 서버로 개인정보가 업로드되지 않더라도 개별 기기 차원에서 기계학습 모델의 학습이 가능하도록 하는 방법이다.[13] 기계학습의 일정한 패러미터만 개별 기기로부터 서버로 전송이 되도록 하여, 개별 기로부터 서버에 집중되는 데이터 자체를 최소화하는 방식을 통해 프라이버시의 보호를 달성하고자 하는 것이다. 최근에는 연합학습의 과정에 DP 개념을 적용하여 프라이버시가 더욱 강력하게 보호될 수 있도록 하는 방법론이 제안되기도 하였다.[14]

12 Min-Jeong Park and Hang J. Kim, “Statistical disclosure control for public microdata: present and future”, 29(6) The Korean Journal of Applied Statistics 1041, 1052-1055 (2016).

13 Jakub Konečný et al., “Federated learning: Strategies for improving communication efficiency”, arXiv:1610.05492v2 [cs.LG] 1, 1-3 (2017).

14 Robin C. Geyer et al., “Differentially private federated learning: A client level perspective”, arXiv:1712.07557v2 [cs.CR] 1, 2-3 (2018).

## 2. DP는 무엇을 의미하는가?

개인정보의 보호와 관계된 국내외 법령은 흔히 개인정보의 의미를 규정한 뒤 이로부터 개인정보의 처리에 관한 원칙과 법률적 근거를 정하는 구조를 가진다. 우리나라의 개인정보 보호법도 마찬가지다. 개인정보는 식별가능성(identifiability) 및 결합가능성(linkability)을 핵심적인 개념 지표로 하여 규정된다. "식별"은 타인과 구별하여(singling-out) '알아볼 수' 있는 정보주체의 고유한 속성이 존재하는 것을 전제로 하는 것이고, "결합가능성"은 개인정보가 보조정보(auxiliary information) 등 부가적인 다른 정보와 연결될 수 있는 가능성을 말하는 것이다.[15] 식별의 개념과 관련하여, 법률에 규정된 '개인을 알아본다'는 것의 정확한 의미가 무엇인지에 관해 법률에 더 구체적인 개념규정이나 설명이 포함되어 있지는 않다(개인정보 보호법 제2조 제1호).

개인정보의 법적 개념 특히 식별의 개념이 충분히 명확하지 않다는 문제제기는 국내뿐 아니라 외국에서도 볼 수 있는 것이다. 우선, 식별과 결합의 개념으로 개인정보의 개념을 구성할 경우에 개인정보의 법적 의미는 불명확한 면이 있고, 그로 인해 현실적으로 프라이버시 보호의 범위가 제한될 가능성이 있다는 시각이 있다.[16] 우리나라의 개정 개인정보 보호법상 개인정보는 합리적으로 식별이 가능한 정보를 말한다(개인정보 보호법 제2조 제1호, 제58조의2). 그런데 '합리적으로 식별가능하다'는 것이 무엇을 의미하는지 더욱 구체적으로 규정하거나 사전적으로(ex ante) 설명하기는 쉽지 않다. 또한, 실제로 개인정보를 처리하는 방법은 개별 분야의 특수성 그리고 처리의 상황이나 맥락에 따라 다를 수 있다는 점을 고려해야 할텐데, 법체계가 이를 고려하기 어렵게 한다는 시각도 있다. 예를 들어, 생명윤리 및 안전에 관한 법률에서 규율하는 '인간대상연구'는 생명윤리와 관계된 것이고, 이 법의 규율대상인 경우에는 정보주체의 동의가 있더라도 그와 관계없이 기관생명윤리위원회의 심의가 필요할 수 있다. 좀 더 회의적인 시각에서는, 개인정보 처리의 기본원칙과 법률적 요건이 준수된다고 하더라도 프라이버시가 적절히 보호되기 어려울 수도 있다는 주장이 나타나기까지 한다.[17]

이러한 한계와 어려움을 고려하여, Dinur & Nissim는 개인정보의 개념 자체보다는 개인정보의 보호가 가지는 의미에 집중하는 것이 유용하다고 보았다. 이들은 프라이버시의 침해가능성으로부터 역으로 개인정보의 보호가 가지는 의미를 확인할 수 있을 것으로 보았다. 따라서 데이터를 보유한

15 개인정보의 개념 지표에 관하여, 식별이 구별과 동일한 의미를 가지고 있다는 시각도 있고, 그에 더하여 정보주체의 신원정보가 요구된다는 시각도 있다. 채성희, "개인정보의 개념에 관한 연구-식별가능성에 관한 유럽 및 일본의 논의를 중심으로", 석사학위 논문, 서울대학교 (2017), 127-131.

16 Paul M. Schwartz & Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 N.Y.U. L. Rev. 1814, 1829-30 (2011).

17 Kobbi Nissim and Alexandra Wood, supra note 2, 3-6.



'큐레이터'가 데이터 이용자에게 데이터를 이용한 연산의 결과를 제공한다고 가정한 다음에[그림 1], 그 결과로부터 개인정보가 복원될 수 있다면 개인정보의 침해가 발생한 것으로 보고 분석모형을 마련하였다. 이때 변환된 데이터로부터 개인정보를 복원하기 위한 시도를 '재구성 공격(reconstruction attack)'이라고 부른다. 한편 재구성 공격이 성공할 가능성과 관련하여, 큐레이터가 상당한 정도로 변조된 데이터를 데이터 이용자에게 제공한 경우가 아니라면, 개인정보의 복원을 통한 프라이버시 침해가 가능한 경우가 많다는 것이 이들의 연구에 의해 밝혀졌다.[18] 예를 들어, <표 1>에 제시된 가상의 결과로부터 거꾸로 계산을 하여 데이터베이스에 담겨있는 개인들에 대한 속성정보의 파악이 가능하다는 것이다. 즉, <표 1>에서 출발하여 <표 2>의 결과를 복원하는 것이 가능하다는 것이다. 이러한 방법론과 별개로, 주어진 데이터베이스에 특정 정보주체에 관한 정보가 포함되어 있는지 확인하는 방식의 기법이 연구되기도 하였다. 이와 같은 기법은 '구성원 공격(membership attack)'이라고 불리는 것이다.[19] 구성원 공격을 통해 특정 정보주체에 관한 정보가 해당 데이터베이스에 포함되어 있는지 파악할 수 있다면 이 또한 프라이버시 침해가 나타나는 한 형태라고 볼 수 있다.[20]

18 Irit Dinur and Kobbi Nissim, "Revealing information while preserving privacy", Revealing information while preserving privacy 202, 202-204 (2003).

19 Homer et al., "Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays", 4(8) PLoS genetics 1, 7-9 (2008).

20 이와 별개로, 좀 더 직접적으로 (재)식별을 시도하는 방식의 연구도 있다. Narayanan & Shmatikov는 Netflix가 공개한 데이터와 IMDB를 통해 입수가능한 데이터를 연결하는 방식의 시도를 통해, 결과적으로 일부 정보주체의 신원을 확인해 낸 연구결과를 제시하였다. Arvind Narayanan and Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets", 2008 IEEE Symposium on Security and Privacy, 111, 118-123 (2008). 이를 '재식별 공격(re-identification attack)'이라고 부를 수 있다. 재식별 공격은 개인정보의 의미와 직접적으로 연관된 것으로, 그동안 적지 않은 공학적 연구와 논의가 이루어졌다.

| Statistic | Group | Count | Median Age | Mean Age |
|---|---|---|---|---|
| 1A | Total Population | 7 | 30 | 38 |
| 2A | Female | 4 | 30 | 33.5 |
| 2B | Male | 3 | 30 | 44 |
| 2C | Black | 4 | 51 | 48.5 |
| 2D | White | 3 | 24 | 24 |
| 3A | Single Adults | (D) | (D) | (D) |
| 3B | Married Adults | 4 | 51 | 54 |
| 4A | Black Female | 3 | 36 | 36.7 |
| 4B | Black Male | (D) | (D) | (D) |
| 4C | White Male | (D) | (D) | (D) |
| 4D | White Female | (D) | (D) | (D) |
| 5A | Person Under 5 Years | (D) | (D) | (D) |
| 5B | Person Under 18 Years | (D) | (D) | (D) |
| 5C | Person 64 Years Or Over | (D) | (D) | (D) |

<표1> 인구 통계 정보[21]

| Age | Sex | Race | Marital Status |
|---|---|---|---|
| 8 | F | B | S |
| 18 | M | W | S |
| 24 | F | W | S |
| 30 | M | W | M |
| 36 | F | B | M |
| 66 | F | B | M |
| 84 | M | B | M |

<표2> 복원 개인정보[22]

21 이것은 인종과 성별, 나이, 결혼 여부 등이 포함된 가상의 사례다. 부분적으로 마스킹 기법이 사용되었다. Simson L. Garfinkel et al., "Understanding Database Reconstruction Attacks on Public Data", 16(5) ACM Queue 1, 6-17 (2018).

22 <표 2>의 내용은 <표 1>을 통해 제시된 인구통계 정보로부터 도출할 수 있는 유일한 해(solution)이다. 현실적으로 가능한 상황은 어떠할지 확대해서 생각해 보면, 이와 유사하게 부분 마스킹 처리가 이루어진 데이터베이스로부터 다수의 해들이 추출될 수 있는 경우가 종종 있을 수 있다. 유일한 해가 존재하지 않는 경우에도 확률적 추론은 가능할 수 있고, 확률적 추론만으로도 프라이버시 침해가 발생할 가능성이 있다. id., 6-17.



미국 인구조사국에서 최근에 수행한 실험은 재구성 공격의 현실적 가능성에 대해 확인해 주었다. 이 실험에 의하면, '데이터 교환(data swapping)'의 방법을 이용하여 변환이 이루어진 2010년 인구조사의 결과로부터 308,745,583명 가운데 46%에 달하는 142,000,000명의 정보주체에 대한 개인정보가 복원되었다. 그리고 연령에서의 약간의 오차(±1년) 가능성까지 포함하여 좀 더 넓게 고려하면, 71%에 달하는 219,000,000명의 정보주체에 대해 개인정보의 복원이 가능하였다. 또한 138,000,000명(45%)의 개인정보가 상업적으로 공개된 데이터베이스를 통해 연결가능하였고, 이 중에서 38%인 52,000,000명의 정보주체에 대해서는 신원정보의 확인이 가능하였다.[23] 이와 같은 정보 복원의 가능성으로 인해, 데이터 이용자에게 일정 수준 이상의 정확도가 담긴 변환 데이터가 제공된다면 이로부터 전체 데이터베이스의 내용이 상당부분 정확하게 노출될 수 있기 때문에 결국 프라이버시 침해가 발생하게 될 상당한 리스크가 있다고 보는 시각도 있다.[24]

이와 같은 연구의 흐름 속에서, 개인정보 보호의 의미가 수학적으로 규정될 필요가 있다고 보고 개념정립을 시도한 연구자들이 나타났다.[25] Cynthia Dwork 교수는 프라이버시에 관한 수학적 개념의 정립에 있어 중요한 역할을 하였는데, Dwork 교수는 개인정보의 처리를 통한 효용(utility)의 달성이라는 목적과 보조정보(auxiliary information)의 가용성 등을 중심적으로 고려하여 개념정립을 해야 할 것으로 보았다.[26] 그녀는 데이터 이용자에게 제공된 결과로부터 직접 정보주체와 관련된 새로운 정보를 추출해 내지 못하도록 하는 방식의 기준만으로는 프라이버시 보호가 충분하지 않을 수 있다고 보았다. 특히, 새로운 정보의 취득가능성을 높여주는 보조정보가 존재할 가능성이 있기 때문에 이를 고려해야 한다는 것이다.

이러한 방식의 개념규정이 어떤 것인지 직관적으로 이해하기 위해, 가상의 사례를 통해 생각해 보자. 개인정보를 보유한 큐레이터가 데이터 이용자에게

23 Michael Hawes, "Title 13, Differential Privacy, and the 2020 Decennial Census", Title 13, Differential Privacy, and the 2020 Decennial Census (2019. 11. 13.), 11-19.

24 "Too many statistics published too accurately from a confidential database exposes the entire database with near certainty."John M. Abowd, "The U.S. Census Bureau Adopts Differential Privacy", 24th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (2018. 8. 23.), 9.

25 Nissim et al., supra note 2, 697-699

26 Cynthia Dwork 교수는 다음의 의문을 제기하였다. "What constitutes a failure to preserve privacy? What is the power of the adversary whose goal it is to compromise privacy? What auxiliary information is available to the adversary (newspapers, medical studies, labor statistics) even without access to the database in question? Of course, utility also requires formal treatment, as releasing no information or only random noise clearly does not compromise privacy".

연산의 결과를 제공한다고 가정해보자. 구체적으로, 리투아니아 여성의 평균 신장이라는 상당히 일반적인 통계치가 제공된다고 하자. 만일 데이터 이용자에게 "데이터셋에 포함된 Terry Gross의 신장은 리투아니아 여성의 평균보다 2인치가 작다"는 보조정보가 존재하는 상황이라면, 리투아니아 여성의 평균 신장이라는 일반적인 데이터를 통해서도 Terry Gross 라는 구체적인 정보주체의 신장이 공개되는 것이나 다름없는 결과가 나타날 수 있다.[27] 또한 이러한 결과는 Terry Gross가 자신에 관한 개인정보의 수집이나 공개를 거부하더라도 발생할 수 있다. 정보주체는 본인에 관한 개인정보의 처리와 관련하여 자기결정권을 가지는 것이 중요한 원칙인 것으로 흔히 언급된다. 그와 동시에, 제3자에 관한 개인정보의 처리와 관련된 의사결정을 할 수 있는 권리는 해당 제3자에게 주어지는 것이 원칙이다. 이러한 원칙을 고려하면, Terry Gross의 사례에서 해당 개인의 개인정보가 실질적으로 공개되는 결과가 발생하는 것은 불가피한 면이 있다. 다만, 개인정보의 처리를 거부한 정보주체도 개인정보를 이용하여 달성할 수 있는 사회적, 경제적 이익을 공유하게 될 수 있다는 점에서 이러한 현상이 발생할 가능성이 정당화될 수 있다는 주장을 할 수는 있다.[28]

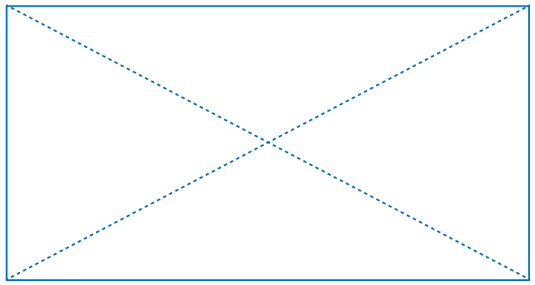
Cynthia Dwork 교수는 이상의 논의를 통해 프라이버시 보호의 수준을 정하는 기준을 마련하였다. 정보주체가 개인정보의 수집을 동의한 경우(real-world scenario)에도 수집을 거부한 경우(opt-out scenario)에 준하는 정도의 프라이버시 보호가 제공되어야 하는 것으로 보고 기준을 정해야 한다는 것이 핵심 아이디어였다. 여기서 프라이버시 보호의 정도를 규정하는 척도를 수치화하여 'ε' 이라 표시할 수 있고, 이 때 이 개념을 'ε-DP'라고 부른다. DP 개념의 적용을 통해 보호된 정보주체의 프라이버시는 개인정보의 수집을 거부한 경우와 비슷한 정도의 프라이버시 보호를 받게 된다.[29] [그림 2]는 DP 개념을 그래프를 통해 표시한 것이다. 이 그림은, 두 개의 그래프를 통해 DP 개념이 적용된 경우와 그렇지 않은 경우 사이의 차이에 질의(query)에 대한 응답의 차이가 일정한 범위 이내에 머무르는 것을 보여주는 것이다.

27 Cynthia Dwork, supra note 9, 1-3.

28 Nissim et al., supra note 2, 230-232.

29 Cynthia Dwork, id. 8-9.



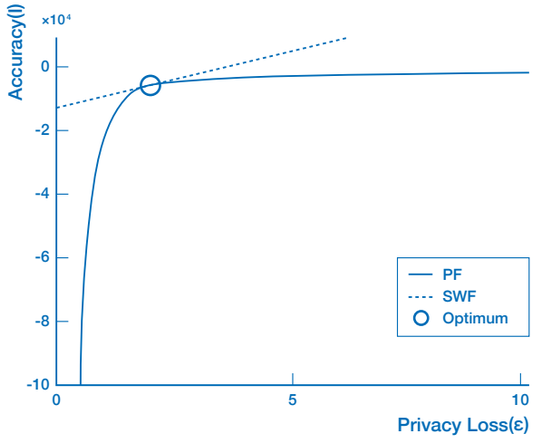


[그림 2] DP 분포[30]

ε-DP는 프라이버시 보호의 정도가 상수 ε의 값에 의해 정해진다는 것을 가리킨다. 이 값을 '프라이버시 예산(privacy budget)'이라고도 부른다. ε 값이 감소한다면 프라이버시가 더 강조되는 것이고, 반대로 ε 값이 증가한다면 개인정보의 활용가능성이 상대적으로 더 강조되는 것이다. 따라서 DP 개념의 구현에 있어, 현실적으로는 ε 값을 어떻게 설정할 것인지가 매우 중요하다. 실제로 DP 개념이 적용될 경우 ε 값을 데이터 이용자나 정보주체에게 공개해야 하는지에 관한 논란도 있다. ε 값이 공개되더라도 공개 자체가 개인정보의 보호 수준에 영향을 미치게 되는 것은 아니기 때문에 투명성과 정당성 확보를 위해서는 이 값을 공개할 필요가 있다는 시각이 있는 한편, 이 값을 공개하면 이 값 자체를 둘러싼 논란이 커질 수 있으므로 공개에 따른 부작용을 고려해야 한다는 시각도 있다. 이처럼 서로 다른 시각이 나타나게 되는 기본적인 이유는, ε 값의 결정이 개인정보의 활용으로부터 발생하는 가치와 프라이버시 보호의 가치 사이에서 적절한 균형을 찾는 일종의 사회적 선택의 문제(social choice problem)이기 때문이다. 즉, 일단 ε 값이 정해지고 나면 엄밀한 수학적 연산을 통해 관련된 수치들이 계산될 수 있지만, ε 값 자체는 사회적 선택 등의 방식으로 외생적으로 결정되어야 하는 것이다. 사회적 선택의 문제에 관한 해법은 주로 법경제학이나 공공경제학의 분석틀을 활용하여 모색할 수 있다. Abowd & Schmutte는 데이터 분석의 정확도에 대한 '지불의향' - 좀 더 정확하게는 "willingness to pay for data accuracy with increased privacy loss" - 을 측정하는 방식을 통하여 최적의 사회적 해법을 찾을 수 있다고 주장하였다[그림 3].[31]

30 Tianqing Zhu et al., "Preliminary of Differential Privacy", Differential Privacy and Applications, 69 Advances in Information Security, Springer International Publishing (2017), 2.

31 John M. Abowd and Ian M. Schmutte, "An economic analysis of privacy protection and statistical accuracy as social choices", 109.1 American Economic Review 171, 194-197 (2019).




[그림 3] 개인정보 보호 예산의 결정 문제[32]

DP 개념의 실제 적용은 개념적으로 두 단계 메커니즘을 이용하여 이루어질 수 있다. 우선 개별 데이터 포인트가 전체 통계 분포에 미치는 영향을 고려하여 약간의 '잡음(noise)'를 데이터베이스에 추가한다. 잡음의 역할은, 해당 데이터베이스에 대한 분석의 결과에 커다란 영향을 미치지 않는 동시에 데이터베이스에 담긴 개개인에 관한 정보가 정확히 드러나는 상황이 발생하는 것을 방지하기 위한 것이다. 두 번째로, 매 질의(query)마다 어느 만큼의 정보가 노출되는지 계산하여 이를 전체 프라이버시 예산에서 차감한다. 이러한 방식으로 프라이버시 예산에 관한 고려를 하여, 일정 단계에 이르면 질의에 대한 응답이 더 이상 제공되지 않도록 통제한다.

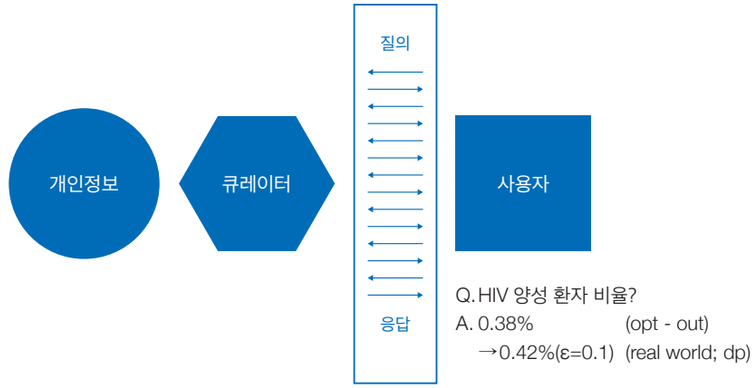
DP 개념이 제시된 이후로 그에 관한 이론적 검증과 보완을 위한 노력이 지속적으로 이루어졌다. 예를 들어, 가우스 메커니즘(Gaussian mechanism)은 ε 값과 관계된 평균과 분산을 가지는 가우스 분포로부터 생성한 임의의 잡음을 더하여(noise addition) 변조된 결과를 데이터 이용자에게 제공할 수 있다.[33] 라플라스 메커니즘(Laplace mechanism)의 경우에는 분산이 개인정보의 민감도(sensitivity)/ε 상수와 비례하도록 설정된 라플라스 분포로부터 생성한 임의의 잡음을 더하여 변조된 결과를 이용자에게 제공할 수 있다[그림 4].[34]

32 John M. Abowd and Ian M. Schmutte, id, 171-174.

33 Cynthia Dwork et al., "Exposed! A Survey of Attacks on Private Data", 4(1) Annual Review of Statistics and Its Application 61, 79-82 (2017). 그러나, 라플라스 메커니즘(Laplace mechanism)의 이용이 더 일반적인 것으로 보인다. Jerome P. Reiter, "Differential Privacy and Federal Data Releases", 6(1) Annual Review of Statistics and Its Application 85, 88-91 (2019).

34 Cynthia Dwork, supra note 9, 9-11.






[그림 4] 질의응답 과정[35]

## 3. DP는 실현이 가능한 것인가?

구글과 애플은 각각 DP 기법을 이용하여 자사의 플랫폼을 이용하는 사용자들의 개인정보를 보호한다고 설명한다. 구글은 2014년 클라이언트 기반으로 DP 방법론을 적용한 RAPPOR(Randomized Aggregatable Privacy-Preserving Ordinal Response) 기법을 개발하였고,[36] DP가 익명처리의 기법으로 사용된다고 명시적으로 설명하였다.[37] 그리고 2019년에는 DP 기법이 적용된 기계학습의 훈련이 가능하도록 하는 라이브러리 함수를 개발하기도 하였다(TensorFlow Privacy).[38] 애플은 사용자 기기로부터 변조된 개인정보를 암호화하여 서버로 전송한다고 발표하였고, 사용자 문서의 형식을 통해 DP 기법이 적용된 개인정보의 내용과 프라이버시 예산의 값을 구체적으로 공개하였다. 발표된 내용의 한 예를 들자면, 이모티콘의 제안과 관계된 프라이버시 보호의 예산은 4(1회/1일)라고 한다.[39]

35 Alexandra Wood et al., "Differential Privacy: A Primer for a Non-Technical Audience", 21(1) Vand. J. Ent. & Tech. L. 209, 272-273 (2018).

36 Úlfar Erlingsson et al., "Rappor: Randomized aggregatable privacy-preserving ordinal response" Proceedings of the 2014 ACM SIGSAC conference on computer and communications security 1, 5-6 (2014).

37 Google, "Google에서 데이터를 익명화하는 방법", 개인정보 보호 및 약관 https://policies.google.com/technologies/anonymization?hl=ko (2020. 5. 10. 확인).

38 Carey Radebaugh and Ulfer Erlingsson, "Introducing TensorFlow Privacy: Learning with Differential Privacy for Training Data", TensorFlow Blog, https://blog.tensorflow.org/2019/03/introducing-tensorflow-privacy-learning.html (2020. 5. 10. 확인).

39 Apple, "Differential Privacy", Protecting your identity https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (2020. 5. 10. 확인).

이처럼 클라이언트 디바이스에 초점을 맞추는 DP 방식은 '지역적 모델(local model)'이라고 불린다. 지역적 모델은 클라이언트 디바이스로부터 변조된 개인정보가 서버로 수집된다는 것이 중요한 특징이다. 그러한 점에서 정보주체의 개인정보가 그대로 서버로 수집되는 '중앙집중형 모델(central model)'과 대비되는 방식이다.[40] 통신 보안을 신뢰할 수 없는 상황이라거나(insecure channel) 데이터 큐레이터를 신뢰할 수 없는 상황이라면(untrusted curator) 서버에 개인정보가 그대로 제공되는 방식이 적절하지 않을 수 있다. 나아가 큐레이터 스스로가 정보주체에 관한 데이터의 습득을 원할 가능성이 있는 경우에도(honest-but-curious curator) 서버에 개인정보가 집중되는 방식이 부적절할 수 있다. 다른 한편, 클라이언트로부터 변조된 개인정보가 수집되는 방식 하에서는, 관련 데이터가 제3자에게 공개되더라도 정보주체의 프라이버시는 사전에 정해진 기준을 충족하면서 계속적으로 보호가 될 것이다. 따라서 통신 채널이나 큐레이터의 신뢰도에 제한이 있는 경우에는 지역적 모델이 유용할 것이다. 반대로 통신 채널 및 큐레이터에 대한 신뢰도가 충분한 경우에는 중앙집중형 모델이 더 유용할 수 있다.

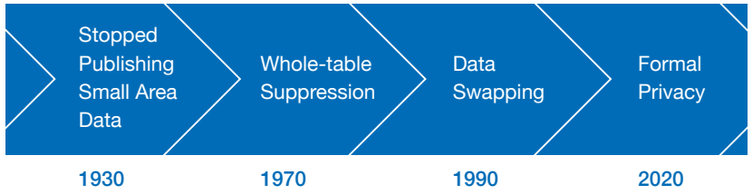
일반적으로 공공영역의 통계작성기관은 신뢰할만한 큐레이터라 볼 수 있다.[41] 그런 점에서 미국의 인구조사(US Census)는 공공영역의 신뢰할만한 큐레이터가 역할을 하는 사례로 참고할만하다. 미국 인구조사국(Census Bureau)은 2020년부터 DP를 적용한 인구조사를 시행한다고 발표한 바 있다. 인구조사에 관한 미국의 법조항은 인구조사로부터 수집된 개인정보가 통계의 목적으로만 이용되어야 한다고 규정하고 있고(13 U.S. Code § 9), 정보주체의 식별이

40 오류의 측면에서, 중앙집중형 모델은 1/ 정도의 오류가 그리고 지역적 모델은 1/ 정도의 오류가 발생한다고 알려져 있다. 즉 중앙집중형 모델이 지역적 모델보다 더 정확한 편이다. 다만, 오류의 크기를 고려할 때, 데이터의 크기가 상당히 큰 경우에는 지역적 모델도 유용하게 활용하는 것이 가능할 것이다.

41 국내에서는 통계법에 통계작성기관을 별도로 규정하고 있다. 통계법에는 "중앙행정기관·지방자치단체 및 제15조에 따라 지정을 받은 통계작성지정기관"이 규정되어 있다(동법 제3조 제3호). 그리고 통계작성기관은 "통계의 작성·보급 및 이용을 촉진하기 위하여 정부정책의 수립·평가 또는 경제·사회현상의 연구·분석 등에 이용되는 수량적 정보를 작성하고 있거나 작성하고자 하는 기관"으로서, 금융기관, 공사, 공단, 연구기관, 협회, 조합, 기타기관 등이 포함된다(동법 제15조 제1항).



가능한 형태의 공표는 허용되지 않는다고 정하고 있다.[42] 인구조사 데이터로부터 프라이버시를 보호하는 방법은 역사적으로 변화의 과정을 거쳐왔는데, 근래에는 데이터 교환(data swapping)의 방법이 주로 이용되었다. 그런데, 위에서 본 것과 같이, 데이터 교환의 기법을 이용하여 데이터의 변환이 이루어진 경우에 개인정보의 복원이 가능할 수도 있다는 연구결과들이 나타나면서, 교환의 방법으로는 프라이버시 보호가 충분하지 않을 것이라는 인식이 형성되었다. 따라서 프라이버시 보호의 방법을 현대화(modernizing its approach to privacy protections) 할 필요가 있다는 논의가 이루어졌고, 검증이 가능하고(verifiable) 측정이 가능한(measurable) 형태의 프라이버시 보호를 제공한다는 점에서 DP가 선택되었다[그림 5].




[그림 5] 미국 인구조사국의 개인정보 보호 방법[43]

다른 한편, 최근 들어 미디어 알고리듬과 민주주의가 중요한 사회적, 정치적 논의의 주제로 대두되면서, 페이스북 등의 소셜 네트워크에 대하여 연구 분석을 위해 이용자 데이터를 제공할 것을 요구하는 목소리가 점점 적극적으로 등장하였다.[44] 이에 페이스북은 Social Science One, Social Science Research Council 등의 조직과 협의체를 구성하여, 2017. 1. 1.부터 2019. 8. 6.사이의

42 원문은 다음과 같다. "(a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, or local government census liaison, may, except as provided in section 8 or 16 or chapter 10 of this title or section 210 of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998 or section 2(f) of the Census of Agriculture Act of 1997 — (1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or (2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or (3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports." 13 U.S. Code § 9 (Information as confidential; exception).

43 Michael Hawes, supra note 22, 7.

44 고학수 외 공저, "민주주의는 위협받고 있는가?: 알고리듬, 프로파일링 시대의 명암", 미디어 알고리듬과 민주주의, 서울대학교 인공지능정책 이니셔티브 (2019. 11. 8.), 20-26.

기간 동안 이용자들 사이에서 공유된 웹 페이지들로 구성된 데이터셋을 마련하여 이를 연구를 위해 제공하기로 하였다. 페이스북의 연구자들은 k-익명성(k-anonymity) 방법을 이용하여 비식별 처리를 하는 것을 우선 고려하였으나, 수학적으로 증명이 가능한 방식의 개인정보의 보호가 제공되어야 한다는 의견이 제시되면서 판단을 변경하였다. 이에 따라 DP 개념이 적용된 표(table) 형식의 결과를 제공하기로 하고, 장기적으로는 연구자들과 상호작용이 가능한 API 의 개발을 진행하기로 하였다.[45]

## 4. DP는 어떠한 한계를 가지고 있는가?

지금까지 DP 방법론이 실제 상황에 적용된 사례를 보면, 보유하고 있는 데이터의 규모가 매우 크고 또한 프라이버시 보호의 인센티브가 상당한 개인정보처리자에 의해 적용된 경우가 대부분인 것을 알 수 있다. DP의 적용으로 인해 개인정보의 직접적인 활용에 비해 효용성이 일정부분 상실될 수밖에 없다는 한계와 함께, DP의 실제 적용을 위해서는 상당한 비용이 소요된다는 현실적인 이유가 함께 작동한 것으로 보인다.

한편, 미국 인구조사국의 연구자들은 여러 가지의 이론적, 현실적 문제에 직면하였다. 이론적인 측면에서 보면, 예를 들어, 인구조사가 전제하고 있는 계층적 구조(hierarchical structure)를 어떻게 고려할 것인지에 관한 이론이나 일정한 불변값(invariant) 설정이 필요할 경우에 어떻게 이를 달성할 수 있을지에 관한 이론은 아직까지 개발된 바 없다는 어려움이 있었다. 또한 인구조사의 결과에 따라 공공 예산의 배분이 영향을 받는 면이 있는데, 소규모 지역사회가 DP의 적용에 따른 불이익을 입지 않도록 분석모형을 조정할 필요가 있을 경우에 구체적으로 어떻게 분석모형을 조정할지에 관한 이론은 아직 마련된 바 없다는 한계도 있었다.[46] 이러한 여러 한계로 인해 상당한 시간과 노력이 수반되는 연구와 논의의 과정이 지속되었다.[47] 이론적인 한계와 별개로 운영상의 현실적 문제도 있었다. 우선 DP의 이론에 익숙한 연구자들이 부족하였다. 그리고 연산과 검증을 위한 도구와 자원도 충분하지 않았다. 데이터의 잠재적 이용자들과 관계된 문제도 있었다. 과거의 이용자들을 보면 인구조사 데이터의 잠재적 이용자들

45 Daniel Kifer et al., "Guidelines for Implementing and Auditing Differentially Private Systems", ArXiv:2002.04049 [Cs] 1, 3-4 (2020); European Data Protection Supervisor, "A Preliminary Opinion on Data Protection and Scientific Research", European Data Protection Supervisor (2020. 1. 6.), 9.

46 Simson L. Garfinkel et al., "Issues Encountered Deploying Differential Privacy", Proceedings of the 2018 Workshop on Privacy in the Electronic Society 133, 134-135 (2018).

47 Daniel Kifer, "Consistency with External Knowledge: The TopDown Algorithm", Data Privacy: From Foundations to Applications, Simons Institute (2019. 3. 4.), 4-9.



중에는 외부의 연구자들이 적지 않고, 이들은 개인정보를 가공한 결과보다는 개인정보가 포함된 로데이터(raw data)를 필요로 하는 경우가 많다는 특징이 있다. 그런데 인구조사국 입장에서는 개인정보가 포함된 데이터를 제3자에게 제공하는 경우에 프라이버시 보호에 커다란 제약이 있을 수밖에 없다는 전제 하에, 데이터를 변형하여 제공하거나 기타의 방식을 통해 제한적으로 제공할 수밖에 없을 것이라는 어려움이 있다.[48] 이와 별도로 데이터 이용자들이 프라이버시 보호의 의미와 데이터 변조의 의미를 오해하여 받아들일 가능성에 관한 우려가 제기되기도 하였다.[49]

기업의 경우에, 최근 논의가 많이 이루어진 페이스북 사례를 보면 산업적으로 이용이 가능한 그리고 확장이 가능한(scalable) 방식의 프라이버시 보호는 기존의 방법을 통해서는 달성이 어려울 수 있다는 인식과 함께, 결국은 상호작용이 가능한 API 개발이 필요할 것이라는 논의가 이루어졌다.[50] 페이스북의 작업에 관여한 연구자들은, 장기적으로 시스템 설계가 코드의 분석과 테스트 요소를 포함한 것이어야 한다고 제안하였고, 연산을 최소화하고 오류의 발생을 감소시키기 위하여 모듈화(modularity) 설계가 필요하다고 제안하였다. 이를 위해, 프라이버시 층(privacy layer), 사용자 인터페이스 및 후처리 층(user interface, postprocessing layer), 액세스 층(data access layer)으로 구조를 분리하여 생각할 필요가 있다는 제언을 하였다. 이와 같은 방식으로 구조를 분리하여 고려하는 것은, 데이터를 그대로 이용가능하게 하는 방식(off-the-shelf mechanism)은 사실상 찾기 어렵다는 판단을 전제로 하는 것으로 볼 수 있다.

DP 방법론을 적용할 경우에 개인정보의 사회적, 경제적 의의의 상당한 부분이 상실될 가능성이 있다는 점도 한계이다. 예컨대, 구글은 RAPPOR 기법을 대신하고자 시스템 아키텍쳐(Enconde, Shuffle, Analyze) 및 그것이 실현된 PROCHLO 기법을 개발하였다. 구글의 연구자들은 개인정보의 변조로부터 상대적으로 미미한 신호가 상실된다는 사실을 확인하였다. 한편으로는 데이터가 가지는 통계적 성격(statistical nature) 그리고 불분명(opaque)하고 경직된(fixed) 성격이 개발자들의 분석을 어렵게 한다는 점도 지적되었다.[51]

48 예컨대, 인구조사와 관계된 개인정보의 이용은, 연구의 내용과 방법론(methodology), 그리고 이용할 개인정보의 내용과 기간을 포함한 설명(project description)과 연구의 이익(benefit statement)을 기술한 제안서(research proposal)를 제출하여, 해당 제안서에 대한 심사로부터 적합하다는 판단을 받아야 한다고 규정하였고, 또한 FSRDC(Federal Statistical Research Data Centers)에서의 이용만 가능하다고 규정하였다.

49 Simson L. Garfinkel et al., supra note 27, 135-136.

50 Daniel Kifer et al., supra note 23, 9-13.

51 Andrea Bittau et al., "PROCHLO: Strong Privacy for Analytics in the Crowd", Proceedings of the 26th Symposium on Operating Systems Principles 441, 442-444 (2017).

애플의 경우에는 DP와 관계된 소스코드의 내용과 설정된 프라이버시 예산의 크기가 어떠한지를 외부에 공개하지 않는다는 비판적 시각이 있어왔다. 결국 일부 연구자들은 리버스 엔지니어링을 통해 애플이 설정한 프라이버시 예산의 크기를 밝혀냈고, 이를 통해 프라이버시 예산이 지나치게 높은 수준에서 설정된 것 아닌가 하는 문제제기를 하기도 하였다.[52] 프라이버시 예산의 크기가 크다면 이는 개인정보가 대부분 변조되지 않고 유지된다는 의미이므로 프라이버시 리스크가 큰 것 아닌가 하는 문제의식을 반영한 것이다.

한편, 13 U.S. Code § 9 조항이 정하는 개인정보의 보호와 DP를 통한 개인정보의 보호는 서로 다른 의미를 가지는 것이라는 주장이 나타나기도 하였다. 그러한 맥락에서, 재구성 위험이나 재식별 위험에 관한 논의는 현실을 과대평가하는 것이고, 무엇보다도 인구조사국은 정확한 데이터를 외부에 제공하여야 하는 의무가 존재하는데, DP 개념의 도입을 통해 인구조사국이 이를 무시하는 결정을 한 것이라는 주장이 제기되었다.[53] 이와 관련된 맥락에서, El Emam 교수는 개인정보를 이용한 차별을 제한하는 것이 프라이버시 보호의 중요한 목적이라고 주장하였다. 그에 따라, 개인정보의 이용과 제공 자체에 집중하기 보다는 관련된 의사결정에 관한 규범적 통제가 더 중요할 수 있다는 취지의 주장을 하였다.[54] El Emam 교수는 재구성 공격이나 재식별 공격이 성공한 실제의 사례는 찾아보기 어렵다고 주장하기도 하였다.[55]

## 5. 결론

DP는 프라이버시 보호에 관하여 그 척도를 수학적으로 개념을 정의하여 응용하는 것이다. 그런데 이러한 방식으로 개인정보의 보호에 관해 규정하는 것은 법규범을 통해 개인정보를 정의하고 그에 관해 규율하는 방식과는 상당히 다른 것이다. 따라서 DP 개념의 적용을 통한 개인정보 보호의 방식과 법규범의 해석과 적용을 통한 개인정보 보호의 방식 사이에 어떤 차이가 있는지에 대해 명확히 파악하고 비교할 필요가 있다. DP는 법규범상으로는 추상적 판단의 대상으로만 고려되기 쉬운 개인정보 활용으로부터의 효용성과 정보주체의 프라이버시 보호를 통해 달성될 수 있는 가치 사이의 상충관계에 관하여 측정가능한 형태의 개념설정과 이론을 제공한다는 점에서 유용하다. 그러나 프라이버시 예산의 설정을 둘러싼 논란이 발생할 수 있고 또한 이를 구현하는 과정에서 상당한 비용이 소요된다는 한계가 존재하기도 한다.

견고한 프라이버시 보호는 공학적 방법론과 법학을 통한 규범적 논의가 서로 적절한 보완적 역할을 할 때 달성될 수 있다. 따라서 법규범의 마련과 적용에 있어서도 공학적 논의의 가능성과 한계를 적극적으로 파악하고 고려할 필요가 있다. 그러한 맥락의 연구의 한 예를 들면 미국에서는 법학과 컴퓨터공학 분야의 연구자들이 협업하여, DP가 FERPA(Family Educational Rights and Privacy Act of 1974) 규정이 설정한 보호의 기준에 부합하는지에 관하여 연구가 이루어진 바 있다.[56] 이들은 개인정보 보호의 과학적 방법이 법규범이 정한 기준을 준수하는지 확인하여야 한다고 주장하였고, 이러한 확인은 과학과 법학의 공동의 언어와 논증 과정을 통하여 달성될 수 있다고 설명하였다. 미국 인구조사국의 사례나 Harvard Privacy Tools Project 사례 등도 참고할 만하다. 나아가 DP 개념이 좀 더 적극적으로 수용되기 위해서는 가이드라인(guidelines)이나 성공적 사례(best practices) 등이 작성되고 활용되어야 할 것이다.

52 Tang et al., “Privacy Loss in Apple’s Implementation of Differential Privacy on MacOS 10.12” arXiv:1709.02753v2 [cs.CR] 1, 6 (2017). 이것은 연구자들이 확인한 것보다 큰 값이다.

53 Ruggles et al, supra note 10, 406-407.

54 Khaled, El Emam and Cecilia Alvarez, supra note 10, 77-78.

55 Khaled El Emam et al., “A Systematic Review of Re-Identification Attacks on health Data”, 6(12) PLoS ONE e28071, 5-8 (2011).

56 Nissim et al., supra note 2, 763-772.

## 참고문헌


- 고학수 외 공저, “민주주의는 위협받고 있는가?: 알고리듬, 프로파일링 시대의 명암”, 미디어 알고리듬과 민주주의, 서울대학교 인공지능정책 이니셔티브 (2019. 11. 8.).

- Andrea Bittau et al., “PROCHLO: Strong Privacy for Analytics in the Crowd”, Proceedings of the 26th Symposium on Operating Systems Principles 441 (2017).
- Alexandra Wood et al., “Differential Privacy: A Primer for a Non-Technical Audience”, 21(1) Vand. J. Ent. & Tech. L. 209 (2018).
- Apple, “Differential Privacy”, Protecting your identity https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (2020. 5. 10. 확인).
- Arvind Narayanan and Vitaly Shmatikov, “Robust De-Anonymization of Large Sparse Datasets”, 2008 IEEE Symposium on Security and Privacy, 111 (2008).
- Carey Radebaugh and Ulfer Erlingsson, “Introducing TensorFlow Privacy: Learning with Differential Privacy for Training Data”, TensorFlow Blog, https://blog.tensorflow.org/2019/03/introducing-tensorflow-privacy-learning.html (2020. 5. 10. 확인).
- Cynthia Dwork, “Differential Privacy”, Automata, Languages and Programming, Springer Berlin Heidelberg (2006).
- Cynthia Dwork et al., “Exposed! A Survey of Attacks on Private Data”, 4(1) Annual Review of Statistics and Its Application 61 (2017).
- Daniel Kifer, “Consistency with External Knowledge: The TopDown Algorithm”, Data Privacy: From Foundations to Applications, Simons Institute (2019. 3. 4.).
- Daniel Kifer et al., “Guidelines for Implementing and Auditing Differentially Private Systems”, ArXiv:2002.04049 [Cs] 1 (2020).
- European Data Protection Supervisor, “A Preliminary Opinion on Data Protection and Scientific Research”, European Data Protection Supervisor (2020. 1. 6.).
- Google, “GOOGLE에서 데이터를 익명화하는 방법”, 개인정보 보호 및 약관 https://policies.google.com/technologies/anonymization?hl=ko (2020. 5. 10. 확인).
- Homer et al., “Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays“, 4(8) PLoS genetics 1 (2008).
- Irit Dinur and Kobbi Nissim, “Revealing information while preserving privacy”, Revealing information while preserving privacy 202 (2003).
- Jakub Konečný et al., “Federated learning: Strategies for improving communication efficiency”, arXiv:1610.05492v2 [cs.LG] 1 (2017).
- Jerome P. Reiter, “Differential Privacy and Federal Data Releases”, 6(1) Annual Review of Statistics and Its Application 85 (2019).
- John M. Abowd, “The U.S. Census Bureau Adopts Differential Privacy”, 24th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (2018. 8. 23.).
- John M. Abowd and Ian M. Schmutte, “An economic analysis of privacy protection and statistical accuracy as social choices”, 109.1 American Economic Review 171 (2019).
- Khaled El Emam and Cecilia Alvarez, “A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques”, 5(1) International Data Privacy Law 73 (2015).
- Khaled El Emam et al., “A Systematic Review of Re-Identification Attacks on health Data”, 6(12) PLoS ONE e28071 (2011).
- Kobbi Nissim and Alexandra Wood, “Is Privacy Privacy?”, 376(2128) Phil. Trans. R. Soc. A 1 (2018).
- Michael Hawes, “Title 13, Differential Privacy, and the 2020 Decennial Census”, Title 13, Differential Privacy, and the 2020 Decennial Census (2019. 11. 13.).
- Min-Jeong Park and Hang J. Kim, “Statistical disclosure control for public microdata: present and future”, 29(6) The Korean Journal of Applied Statistics 1041 (2016).
- Nabil R. Adam and John C. Worthmann, “Security-Control Methods for Statistical Databases: A Comparative Study”, 21(4) ACM Comput. Surv. 515 (1989).
- Nissim et al., “Bridging the Gap Between Computer Science and Legal Approaches to Privacy”, 31(2) Harv. J.L. & Tech. 687 (2018).
- Nabil R. Adam and John C. Worthmann, “Security-Control Methods for Statistical Databases: A Comparative Study”, 21(4) ACM Comput. Surv. 515 (1989).
- Office of Federal Statistical Policy and Standards, “Report on Statistical Disclosure and Disclosure Avoidance Techniques”, U. S. Department of Commerce (1978).
- Paul M. Schwartz & Daniel J. Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, 86 N.Y.U. L. Rev. 1814 (2011).
- Robin C. Geyer et al., “Differentially private federated learning: A client level perspective” arXiv:1712.07557v2 [cs.CR] 1 (2018).
- Ruggles et al, “Differential Privacy and Census Data: Implications for Social and Economic Research,” 109 AEA Papers and Proceedings 403 (2019).
- Simson L. Garfinkel et al., “Understanding Database Reconstruction Attacks on Public Data”, 16(5) ACM Queue 1 (2018).
- Simson L. Garfinkel et al., “Issues Encountered Deploying Differential Privacy”, Proceedings of the 2018 Workshop on Privacy in the Electronic Society 133 (2018).
- Tang et al., “Privacy Loss in Apple’s Implementation of Differential Privacy on MacOS 10.12” arXiv:1709.02753v2 [cs.CR] 1, (2017).
- Tianqing Zhu et al., “Preliminary of Differential Privacy”, Differential Privacy and Applications, 69 Advances in Information Security, Springer International Publishing (2017).
- Úlfar Erlingsson et al., “Rappor: Randomized aggregatable privacy-preserving ordinal response” Proceedings of the 2014 ACM SIGSAC conference on computer and communications security 1 (2014).

## 서울대학교
## 인공지능정책
## 이니셔티브 안내

서울대학교 인공지능정책 이니셔티브는 인공지능과 관련된 다양한 사회경제적, 법적, 정책적 이슈들을 연구하고 논의하기 위해 시작된 서울대학교 법과경제연구센터의 프로그램입니다. '소셜랩(Social Lab)' 개념을 지향하여, 여러 배경과 관심을 가진 분들 사이의 협업과 지속적인 대화를 추구합니다. 서울대학교 법학전문대학원의 고학수 교수와 임용 교수가 함께 이끌고 있습니다.

### 1. 발간문 안내

서울대학교 인공지능정책 이니셔티브의 주요 발간물은 이슈페이퍼와 워킹페이퍼가 있고, 비정기적으로 발간되는 단행본 및 학술행사 자료집 등이 있습니다. 이슈페이퍼와 워킹페이퍼 등의 자료들은 홈페이지를 통해 다운로드 받으실 수 있습니다.

### 2. 행사 안내

서울대학교 인공지능정책 이니셔티브의 주요 행사는 이슈페이퍼를 발표하고 논의하는 행사(상반기 및 하반기 각 1회) 그리고 국내외 연구자들을 초빙하여 진행하는 대규모 국제학술대회(연 1회) 등이 있습니다. 그 이외에 비정기적으로 진행하는 행사들도 있습니다.

### 3. 이슈페이퍼 2020-1

이번 이슈페이퍼는 서울대학교 인공지능정책 이니셔티브의 세 번째 이슈페이퍼로, 2020. 05. 07.에 열린 웨비나 행사를 위해 준비되었습니다.

**http://sapi.co.kr/**