콜로키움

빅데이터와 프로파일링

□ 일시 : 2015년 2월 13일(금) 오후2시 ~ 6시

□ 장소 : 건국대학교 법학전문대학원 모의법정

□ 주최 : 프라이버시워킹그룹

□ 사회 : 한상희 (건국대학교 법학전문대학원)

□ 발표

(1) 프로파일링의 정의 : 오길영 교수 (신경대학교)

(2) 프로파일링의 동의 : 김보라미 변호사 (경실련 소비자정의센터 위원)

(3) 프로파일링의 제한/금지/거부 : 정혜승 변호사 (법무법인 세승)

(4) 인적 평가와 익명화 관련 : 이은우 변호사 (법무법인 지향)

프로파일링의 정의에 대한 소고

오길영
신경대학교 교수, 정보통신법
eclaw@daum.net

Ⅰ. 들어가며

필자가 프로파일링(Profiling)이라는 용어를 처음 접했던 것은, 리눅스(Linux)열풍이 불던 시절에 유닉스(Unix) 사용법을 공부하면서였다. 그랬던 용어를 이제 또다시 만나게 되었으나, 이는 더 이상 기술용어가 아니었다. 보통 기술적인 용어가 사회적 용어로 수용되는 현상은 크게 2가지의 경우로 생각해볼 수 있다. 그 기술이 대단히 유명해져서 범용으로 사용되거나(예를 들어 2G, 3G, LTE 등), 또는 그 기술적인 위험성 때문에 새로운 규제담론의 도마에 오른 경우이다(패킷감청에서의 Packet, 또는 DPI 등). 프로파일링의 경우에는 아직 그리 명확하지는 않으나 아마도 후자의 경우에 해당하는 것으로 짐작이 된다. 소위 빅데이터(Big Data)의 시대에 있어 가장 주요한 상업화 엔진으로 사용되는 것이 프로파일링 기술이라는 점에서, 아마도 순기능보다는 역기능의 제어를 위해 이에 대한 담론이 형성중인 것으로 판단되기 때문이다.

이 글은 아직 제대로 확립되지 못하고 있는 프로파일링의 정의에 대하여, 현재의 수준에서 짧은 검토를 수행하기 위해 작성되는 글이다. 필자의 연구수준도 미완이기는 하지만, 기실 프로파일링에 대한 국제적인 담론의 수준 또한 미완인 상태이다. 빅데이터라는 공룡이 완전한 모습이 연출되지 못하고 있는 현재의 시점에서 그 심장을 해부해내기 위한 논의를 진행한다는 것 자체가 모순일 수 있으나, 그럼에도 불구하고 국제담론의 움직임은 이미 기민하게 진행되는 모습이다. 어쩌면 이렇듯 기술의 진보에 발맞추어 가는 논의가 반드시 필요한 사항인지도 모를 일이다. 따라서 이번의 이 글은 이러한 국제적인 담론의 상황을 짚어보는 정도로 만족하기로 하고, 그 상세에 대하여는 추후의 연구에서 계속 진행키로 마음먹기로 한다.

Ⅱ. 프로파일링의 개념

1. 일반적인 영역에서의 접근

1.1. 범죄학에서의 프로파일링

범죄학은 인간의 행위를 분석하여 법적으로 평가하는 학문이다. 그런데 인간이 가지는 독특한 성격과 행동양식에 따라 그에 의한 범죄 행동도 사회문화적 맥락의 범위에서 개인의 성격에 따른 일정한 행동 패턴을 갖게 된다고 한다. 따라서 구체적인 범죄 행동 패턴을 면밀히 분석한다면 행위자 성격을 비롯하여 직업적 특성, 거주지 특성, 교육 정도, 경제적 상태, 사회연결망, 취미 등과 같은 인구사회학적 변인들의 군을 파악할 수 있다는 것이 범죄학에서의 프로파일링의 출발점이다. 행동과학적 관점에서, 인간의 행동 유형이 행위자의 인격적 특성을 나타내어 마치 지문과 같이 개인마다 독특한 특징을 가진다고 전제하는 것이다. 즉 "행동은 그 사람의 특성을 반영한다"로 정의해 볼 수 있겠다. 만약 특정한 행위를 했을 경우 다양한 환경변이에도 불구하고 그 행위에 투영된 기본 인성, 행동 유형은 일정한 정형을 유지하고 있어서 이를 유형별로 파악할 수 있다는 것이 범죄학에서의 말하는 프로파일링이다. 이는 연쇄살인범의 행동특성을 파악하고 수사에 활용하기 위해 미국 FBI에서 처음으로 그 사용을 시작한 개념이라는 제법 유명한 일화가 있다.[1)]

1.2. 전산학에서의 프로파일링

전산학에서 말하는 프로파일링은 '데이터 프로파일링'(Data profiling)의 준말로 사용되는 것이 일반적이다. 이는 데이터 소스에 대해 일련의 데이터 검사 절차를 수행함으로써 데이터에 관한 중요한 정보와 통계치를 수집하는 것을 말한다. 데이터베이스에 있는 방대한 정보로부터 숨어있는 지식(hidden knowledge)을 자동적으로 추출하는 과정을 의미하는 '데이터 마이닝'(Data Mining)과 혼용되어 사용되는 것이 일반적이기도 하다. 요컨대, 데이터베이스 내에서 어떠한 방법(순차 패턴, 유사성 등)에 의해 관심 있는 지식을 찾아내는 과정으로서 대용량의 데이터 속에서 유용한 정보를 발견하는 과정[2)] 자체를 의미한다. 그 과정은 크게 '발견(Discovery)'과 '검증(Verification)'의 절차로 구성된다. 만약 데이터의 오류발견을 위한 프로파일링을 실시한다면, 데이터의 발견의 절차를 통하여 오류의 가능성이 있는 부정확한 데이터 현상이 발견되고 발견된 현상은 관련 업무 담당자들과 품질 분석가의 협의를 거쳐서 이를 부정확한 데이터로

---

1) 이 단락의 주요한 내용은 <http://www.dspress.org/news/articleView.html?idxno=4760> 검색일: 2015.2.11.에서 인용하였다.

2) 이는 <http://terms.naver.com/entry.nhn?docId=819914&cid=42344&categoryId=42344> 검색일: 2015.2.11.에서 인용하였다.

결정한다. 여기까지가 '발견'이다. 그 다음, 결정된 부정확한 데이터 규칙과 정확한 데이터 규칙을 토대로 다시금 해당 데이터베이스를 조사하여 오류데이터 내역을 추출하거나 검증하는 행위를 진행하는데 이를 '검증' 또는 데이터 감사(Data Auditing)라고 한다. 요컨대 전산학에서의 데이터 프로파일링은, 데이터의 구조·내용·품질을 발견하고 개선하기 위해 시행되는 다양한 분석 기술을 말한다.[3)]

1.3. 정보학에서의 프로파일링

정보학에서 말하는 프로파일링은 'Dataveillance'라는 용어를 생각하면 접근이 쉽다. 이는 'data'와 'surveillance'가 합쳐져 탄생한 신조어로서, 그 표현 그대로 '데이터 감시(능력)'이라는 의미를 가진다. 이러한 'Dataveillance'를 수행하는 기술을 '프로파일링'이라고 한다.[4)] 이러한 표현은 이미 90년대부터 등장한 것으로 파악된다.[5)] 즉 '정보검색에 사용하기 위해 특정인에 대한 관심을 현출한 도해'라는 '프로파일'(profile)에 관한 사전적 해석을 근거로, 그러한 프로파일을 만들거나 사용하는 과정을 프로파일링으로 설정한 것이 그 시작이다.[6)] 다시 말해 '특정인의 과거 경험으로부터 추론되어지는 특정한 범주의 특징을 조합하는 기술을 말하거나, 또는 그 특징의 조합과 가장 적합한 개인을 찾기 위해 보유된 자료'를 프로파일링이라고 보는 것이다.[7)] 요컨대 정보학에서 말해지는 프로파일링은 '프로파일 정보의 연속적인 생산 과정으로서, 이를 어떠한 사물이나 사람에게 적용하기 위한 데이터의 개발 기술'[8)]을 의미한다.

그 기법에 대하여는 영미의 격언에서 나오는 '건초더미에서 바늘찾기'(a needle in a haystack)를 활용한 재미있는 설명[9)]이 있다. 프로파일링이란 건초더미에서 (무턱대고) 바늘찾기를 하는 것이 아니라, (처음부터) 건초더미의 모든 건초들 하나하나에 대한 정보를 수집하는 방식이라는 말로 은유적 설명이 시작된다. 수집은 물론 그 수집된 데이터를 저장하고 분석하는 것인데, 이는 발생가능한 위험으로 감지되었으나 아직 알

---

3) 이 단락의 주요한 내용은 <http://www.dqc.or.kr/guideline/3-2-0.html> 검색일: 2015.2.11.에서 인용하였다.

4) Ferraris V./Bosco F./Cafiero G./D'Angelo E./Suloyeva Y., Defining Profiling, Working Paper 1 of the Profiling Project(Protecting Citizens' Right Fighting Illicit Profiling, 2013), 2쪽.

5) "Profiling is a data surveillance technique…": Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance" [1993] JlLawInfoSci 26; (1993) 4(2) Journal of Law, Information and Science 403, <http://www.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.html> 검색일: 2015.2.11, 1쪽.

6) "… the schematic representation of a person's interests for use in information retrieval (Concise Oxford, 1976, p.885). The term 'profiling' refers to the process of creating and using such a profile…": Clarke, Roger, 앞의 글, 2쪽.

7) "Profiling is a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics.": Clarke, Roger, 앞의 글, 2쪽.

8) profiling is a process of construction of a series of information (a profile), which is then applied to something or someone (individual or group) by techniques of data elaboration: Ferraris V./Bosco F./Cafiero G./D'Angelo E./Suloyeva Y., 앞의 글, 3쪽.

9) Gloria González Fuster/Serge Gutwirth/Erika Ellyne, Profiling in the European Union: A high-risk practice, INEX Policy Brief No.10 (2010), 2쪽.

수 없는 그 무언가에 대한 프로파일을 개발하기 위해서이라고 한다. 즉 '드물게(uncommonly) 작음', '드물게(uncommonly) 단단함', '드물게(uncommonly) 날카로움'과 같이 연속되는 건초의 특성을 유형화하여 얻어낸 '프로파일'을, 다시금 건초더미의 모든 건초들 하나하나와 재비교하여 '극도로'(extraordinarily) '작거나 단단하거나 날카로운' 건초에 대해 '잠재적으로 위험'(potentially risky)하다는 꼬리표를 달고, 이 꼬리표가 달린 건초가 바로 '바늘'이 된다는 것이 그것이다. 이를 KDD(Knowledge Discovery in Databases)[10]라고 칭한다.

한편 데이터 마이닝에 대해서는 '방대하게 저장된 디지털 정보로부터 (유의미한) 지식을 끄집어내기 위해 사용되는 연속적인 기술'[11]이라고 설명한다. 데이터 마이닝 기법에 대하여는 '합리적인 의심으로 인한 일반적인 서술'(the usual predicate of reasonable suspicion)을 기반으로 하는 '사안기반의 검색'(subject-based searches) 기법과, 의심대상자의 정체성을 밝히기 위한 데이터 관련성의 예측(능)력에 대한 이론(a theory or theories about the predictive power of data linkages to identify suspicious individuals)을 기반으로 하는 '패턴기반의 데이터 마이닝'(pattern-based data mining) 기법을 언급하고 있다. 결국 이는 전산학에서의 프로파일링에 대한 설명에다 사회학적인 '평가'를 첨가한 것이라 볼 수 있다. 또한 앞서 살펴본 프로파일링에 대한 '은유적 설명'을 다소 기술적으로 언급하고 있는 것에 불과한 것이기도 하다. 따라서 데이터 마이닝이 좀 더 기술적인 색채를 지니고 있다는 점은 부정할 수 없겠으나, 단순히 개념적인 시각으로 볼 때 양자는 큰 문제없이 혼용될 수 있는 용어임을 알 수 있으며, 나아가 양자는 모두 전산학적인 알고리즘의 배경위에 서있다는 것을 확인할 수 있다.[12]

2. 법적인 영역에서의 접근

1.1. '정보보호' 차원에서의 정의

정보보호 차원에서의 프로파일링에 대한 접근은 이미 EU의 데이터보호지침(the Data Protection Directive)에서 시작되었음은 주지의 사실이다.[13] 그러나 여기에는 프로파일링에 대한 명시적인 언급이 없었다. 이에 뒤이어 동일한 견지에서 프로파일링에 대해 본격적인 정의를 시도한 사례로 'GDPR(the Draft General Data Protection Regulation) article 20'에서의 정의규정과 'CoE(the Council of Europe)의 권고문(Recommendation)'에서의 정의규정을 들 수 있다.

---

10) Ferraris V./Bosco F./Cafiero G./D'Angelo E./Suloyeva Y., 앞의 글, 7쪽.

11) "Data mining refers to a series of techniques used to extract intelligence from vast stores of digital information.": Ira S. Rubinstein/Ronald D. Lee/Paul M. Schwartz, Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, The University of Chicago Law Review (2008), <https://escholarship.org/uc/item/2zn4z6q4> 검색일: 2015.2.11, 262쪽.

12) 이에 관한 상세는 Ferraris V./Bosco F./Cafiero G./D'Angelo E./Suloyeva Y., 앞의 글, 7-8쪽.

13) Directive 95/46/EC, article 15에서의 'automated individual decisions' 부분을 말한다.

"automated processing intended to evaluate certain personal aspects relating to this natural person or to analyze or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour" [14]

"automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal references, behaviors and attitudes" [15]

나아가 이를 계수하고 있는 'Article 29 Data Protection Working Party'가 제시한 의견 또한 대동소이하다.

"Profiling means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person' health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements" [16]

이들 정의 규정의 내용을 분석해 보면, 크게 3단의 구조를 가지고 있음을 알 수 있다. 먼저 프로파일링은 결국 자동화된 과정(automated processing, automatic data processing technique)이라는 점, 그리고 그 기법은 분석과 예측(analyze or predict, analysis and prediction)이라는 점, 마지막으로 프로파일링의 대상은 결국 사람(natural person, individual)이라는 점이 그것이다. 이 3가지의 요소를 연결해 보면 '사람을 대상으로 자동화된 분석을 실시하고 이를 통해 다시금 사람에 관하여 예측하는 자동화된 과정'이라고 정의해 볼 수 있겠다. 결국 개념설정의 핵심인자는 '기계(즉 전자적인 수단, electronic means[17])와 사람'의 대립구조와, 사람에 '대한 또는 관한' 과정이라는 점이라고 요약할 수 있다.

이는 결국 프라이버시와 정보보호, 자기결정권과 인간의 존엄, 개인의 진실성과 표현

14) article 20, Proposal for GDPR, 2012.
15) paragraph 1, CM/Rec (2010) 13.
16) Article 29 Data Protection Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation(2013), <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf> 검색일: 2015.2.11, 2-3쪽.
17) Protecting Citizens' Right Fighting Illicit Profiling, Final Report Profiling (2014) <http://www.unicri.it/news/files/Profiling_final_report_2014.pdf>, 검색일: 2015.2.11, 13쪽.

및 거주이전의 자유 등의 기본권적 문제와 밀접한 관련성이 있다. 또한 프로파일링에 대한 우려 즉, 자동화된 처리(automated decisions)에 있어 부정확하거나 의미가 퇴색된 정보, 흠결 또는 오류가 있는 기준값의 설정이 야기하는 불리한 프로파일(negative profile)의 양산이 가져오는 불이익과 차별 그리고 침해 등을 이미 고려하고 있음을 의미하기도 한다.[18)]

1.2. '범주설정' 차원에서의 정의

프로파일링 대상정보의 범주와 관련하여 제한을 설정한 경우가 있다. 먼저 인종차별 금지의 견지에서 프로파일링을 경우로서, ECRI(The European Commission against Racism and Intolerance)의 '일반 정책 권고문'(General policy recommendation)상의 정의가 바로 그러한 경우이다.

> racial profiling shall mean: "The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or ethnic origin, in control, surveillance or investigation activities" [19)]

살피는 바와 같이 국제인권법에서 논해지는 인종, 언어, 종교, 국적 등 '차별'의 기준이 되는 관념들이 프로파일링의 정의에 녹아있으며, 이러한 대상정보를 직간접으로 프로파일링을 하는 것을 금지하고 있다.[20)] 이를 두고 본고에서 논하고 있는 프로파일링과 무관한 것으로 판단할 수도 있겠으나, 그 규정의 내용 가운데 'by collecting data'라는 표현을 명시하고 있음[21)]은 물론 규정 전체를 해석하는데 있어 정보학에서의 프로파일링을 배제할 이유가 없다. 따라서 이는 모든 형태의 프로파일링에 대하여 그 대상정보의 범주 설정에 있어 일반원칙으로 기능하게 된다.[22)]

다음으로는 미국온라인광고업자들의 연합체인 'NAI'(Network Advertising Initiative)의 자율규제에 대한 내용을 담은 FTC(Federal Trade Commission)의 권고문[23)]에 등장하는 정의를 들 수 있다. 미의회에 제출하는 보고서로 작성된 동 권고문은 그 말미에서 다음과 같이 서술하고 있다.

---

18) Protecting Citizens' Right Fighting Illicit Profiling, 앞의 글, 15쪽.
19) paragraph 1, ECRI General policy recommendation No 11, 2007 <http://www.coe.int/t/dlapil/codexter/Source/ECRI_Recommendation_11_2007_EN.pdf> 검색일: 2015.2.11, 4쪽.
20) paragraph 2, ECRI General policy recommendation No 11, 2007.
21) paragraph 1.2, ECRI General policy recommendation No 11, 2007.
22) Ferraris V./Bosco F./Cafiero G./D'Angelo E./Suloyeva Y., 앞의 글, 19쪽.
23) FTC, Online Profiling: A Report to Congress, Part2 Recommendations, 2000 <http://www.steptoe.com/assets/attachments/934.pdf> 검색일: 2015.2.11.

NAI companies will not use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, or social security numbers for profiling.[24]

살피는 바와 같이 식별정보(PII)로서 매우 내밀한 정보, 즉 의료 또는 금융정보, 성적 태도나 성향, 사회보장번호 등을 프로파일링의 대상에서 제외하고 있다. 어찌보면 범주에 대한 제한으로서는 지극히 당연한 것일 수 있겠으나 실은 그리 간단하지만도 않다. 왜냐하면 현재 우리나라에서의 담론은 개인정보의 정의 자체에 묶여있기 때문에 이렇듯 특단의 범주를 설정해야한다는 논의가 없는 것이 사실이고, 나아가 NAI의 경우에도 식별정보만을 그 대상으로 하고 있으므로 비식별화 조치 등으로 쉬이 이러한 제한을 벗어날 수 있기 때문이다.

Ⅲ. 나오며

지금까지의 검토를 진행하면서 필자가 느끼게 된 한가지의 맹점을 밝히면서 글을 마치고자 한다. 프로파일링에 대한 법적인 영역에서의 접근은 프로파일링이 가져올 수 있는 부작용에 대한 법적 평가를 그 비난가능성의 근거로 삼고 있다. 즉 프로파일링이 야기하는 개인적·사회적인 차원에서의 '오류'들이 바로 그것이다. 따라서 이를 방지하기 위해 수단을 마련하거나 프로파일링 자체에 대한 규제로써 법적 대응은 귀결된다.
한편 프로파일링이라는 '행위 또는 처리(processing)', 그 자체가 법적으로 문제가 없는지에 대하여는 여전히 의문이 남는다. 특정한 목적으로 인해 '사람을 대상'으로 하여 분석과 예단을 시행한다는 문제, 즉 '인간의 존엄'과 관련된 이 부분의 이슈는 제대로 고려되지 않는다는 느낌을 지울 수 없다. 범죄학에서 진행되어오는 프로파일링의 경우에도 이와 동일한 문제가 발생하는 것이 사실이다. 그러나 현재 실무에서 사용되는 프로파일링 기법들은 보호되는 공익과 침해되는 사익에 대한 이익형량, 즉 비례의 원칙의 검증을 이미 받은 바 있는 것들이라고 요약할 수 있다.

그러나 빅데이터 환경에 있어서의 프로파일링은 그 상황이 완전히 다르다. 여기서의 프로파일링은 특별한 몇몇 경우를 제외하고는 대체로 데이터 상업화의 기술로 받아들여지기 때문에, 형량의 대상이 되는 '공익'이 존재할 수가 없다는 점이 핵심이다. 예를 들어 맞춤광고를 위해 진행되는 프로파일링은 결국 '사업자의 사익'과 '대상자의 사익'간의 충돌이 존재할 뿐이므로, 아예 비례의 원칙이 등장할 만한 상황이 마련될 수가 없다. 따라서 양자를 유사한 것으로 판단하는 것은 심대한 오류이다.

24) FTC, 앞의 문서, 9쪽.

그렇다면 과연 이러한 사익적 프로파일링을 어떻게 평가해야 하는 것인가 하는 새로운 물음표가 남는다. 즉 사익적 프로파일링 자체에 대한 법철학적인 평가가 필요하다는 것이다. 나아가 이를 위해서는, 사람의 사고와 행태 그리고 그에 부수하는 요소들에 대하여 '분석하고 평가하는 행위'와 그 결과의 '정합성'에 대한 고민, 즉 심리학적 차원에서의 접근이 선행되어야만 할 것이다.

결국, 그야말로 쉽지 않은 문제이자 작지 않은 문제이라는 것이다.

- 감사합니다 -

일반적으로 공개된 개인정보에 대한 법적 해석 정리

김보라미 변호사

Ⅰ. 디지털 시대의 새로운 프라이버시 규범의 요구

디지털 시대에 이용자들이 스스로 만들어 내는 정보의 양은 우리의 예상을 훌쩍 뛰어 넘는다. 매일 1조개의 URL이 새롭게 만들어지고, 20억 개의 검색이 구글을 통해 이루어지고 있으며, 300만개의 트윗대화가 만들어지고 있다.[25] 이러한 정보들은 구글과 페이스북과 같은 관련 기업들에 의하여 광고, 마케팅 목적으로 행하는 대규모 감시를 통하여 축적되어가고 있으며, 이러한 정보들은 다시 정부의 정보기관들에 의하여 시민감시의 수단으로 활용되어가고 있다.[26] 2013년 스노든이 미국 정부의 전세계 시민들을 대상으로 하는 대규모 감시 프로그램인 프리즘에 대하여 폭로한 이후 디지털 시대의 프라이버시 문제제기가 전 세계적으로 폭발적으로 나타난 바 있다. 미국정부는 우방국에 대하여도 무차별적으로 도감청을 하였고, 도감청의 피해자였던 브라질 대통령 지우마 호세프 대통령은 2013. 9. 24. 제68차 유엔총회에서 프라이버시 규범의 재정립을 UN차원에서 다시 정비할 것을 요구하였고[27], 유엔총회에서는 디지털 시대의 프라이버시 결의안이 68/167결의로 통과되기도 하였다.[28] 뒤이어 2014. 6. 미법무부는 미국 시민들을 대상으로 하는 사생활 보호 법적 장치들을 유럽연합의 요구에 부응하여 유럽시민에게도 적용하는 법안을 의회에 회부하기로 약속하기도 한 바 있다.[29] 2014. 9. 디지털 시대의 프라이버시 결의안에 따른 특별보고관의 보고서에 의하면 현재 온라인상의 프라이버시는 말살되었다라고 설명하기까지 하였다.

새로운 시대의 프라이버시 논의 중 가장 논쟁적 이슈 중 하나는 일반적으로 온라인상에 공개되어 있는 개인정보들에 대한 프라이버시 보호범위일 것이다. 이미 헬렌 니센바움은 1997년 논문에서 미국내에서 공개된 개인정보들을 취합하여 데이터베이스를 만들어 판매하려고 시도하였던 로투스 마켓플레이스 사례를 통하여 공개된 사생활 역시 맥락에 따라서는 프라이버시 규범의 범위 내에 포함되어야 하며, 점점 정보들을 수집하고 결합하는 컴퓨터와 네트워크의 힘이 증가함에 다라 개인들은 전례없는 방법으로 전면적으로 노출되는 상황에서는 더욱 그렇다는 점을 강조한 바 있다.[30] 즉, 대용

---

25) Terence craig and Mary E. Ludloff, “Privacy and Big Data”, O’Reilly Media, 2011
26) 댄 실러, 번역 김보희 “스노든 사건 그 후, 격변 속의 디지털 자본주의”, 르몽드 74호, 2014. 10. 30.
27) http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf
28) http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
29) 댄 실러, 번역 김보희 “스노든 사건 그 후, 격변 속의 디지털 자본주의”, 르몽드 74호, 2014. 10. 30.
30) Helen Nissenbaum, "Toward an Approach to Privacy in Public : Challenge of Information

량의 숫자, 그림, 문자 언어등을 포함한 대용량 데이터, 소위 “빅데이터”의 활용이 빈번해진 오늘날 일반적으로 공개된 개인정보는 그 스스로의 위치보다 다른 비정형 정보들과 결합되어 사생활을 침해할 가능성이 더 커지고 있다. 기술의 발전으로 개인정보의 보호범위를 제한적으로 바라보기 어려워진 것이다.

이 시점에 프로파일링의 동의와 관련되어 일반적으로 공개된 개인정보에 대한 동의에 대한 논의가 선행되어야 할 것으로 해석되어 아래에서는 이 점에 대한 외국 입법례와 국내 논의를 정리하는 선에서 발표를 마무리하겠다.

Ⅱ. 일반적으로 공개된 개인정보에 대한 해외 입법례

1. EU의 입법례

가.「개인정보의 처리와 관련한 개인의 보호와 개인정보의 자유로운 이동에 관한 1995년 10월 24일 유럽의회 및 이사회 95/46/EC 지침[31] (이하 "EU 개인정보보호지침")」

(1) 개인정보의 정의 조항

EU 개인정보보호지침에 따르면, 개인정보의 정의는 식별되었거나 식별가능한 자연인(정보주체)과 관련된 정보를 의미하며, 이 때 식별가능한 사람이라 함은, 직간접적으로, 특히 신분증 번호 또는 신체적, 생리적, 경제적, 정신적, 경제적, 문화적 또는 사회적 신원을 특정하는 하나 이상의 참조하여 그 신원을 알 수 있는 자를 의미한다(EU 개인정보 보호지침 제2 a항). EU의 개인정보보호지침의 개인정보 정의에는 일반적으로 공개된 개인정보가 포함된다고 해석된다.

(2) 일반적으로 공개된 개인정보의 처리규정

EU 개인정보 보호지침 제7조는 개인정보가 처리될 수 있는 경우를 6가지로 한정적으로 규정하고 있다. 위 규정에 따르면 (a) 개인정보주체가 명백하게 동의를 한 경우, (b) 정보주체가 당사자인 계약의 이행을 위하거나 계약을 체결하기 전에 정보주체의 요청에 따른 조치를 취하기 위하여 필요한 경우, (c) 관리자가 따라야 할 법적 의무를 준수하기 위하여 필요한 경우, (d) 정보주체의 중요한(vital) 이익을 보호하기 위하여 필요한 경우, (e) 공익목적의 업무를 수행하기 위하여 필요한 경우나, 관리자나 그 정보가 공개된 제3자에게 부여된 공적 권한 행사를 위하여 필요한 경우, (f) 관리자 또

Technology", Ethics & Behavior 7(3), 207-219, 1997

31) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

는 정보가 공개된 제3자의 정당한 이익을 위하여 필요한 경우, 다만 그러한 이익이 제1조 제1항에 따라 보호되어야 하는 정보주체의 기본권과 자유의 이익을 침해하는 경우가 아닌 경우에 개인정보의 처리가 가능하다.

일반적으로 공개된 개인정보의 경우도 개인정보의 범위 내에 포함되므로 위 제7조의 각 항에 적용되는 경우에 한하여 그 처리가 가능하므로 위 6가지 경우에 해당하는지 평가하여야 한다. 다만 위 (a)항부터 (e)항까지 포섭되지 않을 경우 (f)항에 따라 정보관리자의 정당한 이익을 위하여 필요한 경우 등의 일반 요건에 따라 해석할 수 있을 것이다. 빅데이터 산업에서 정보주체의 동의를 받지 않고 일반적으로 공개된 개인정보를 활용하는 경우는 (f)항에 포섭되는지가 주로 쟁점이 될 수 있을 것으로 보인다. 그런데 그간 EU 개인정보보호지침 제7조 제(f)항에서 언급된 제3자의 정당한 이익의 범위는 애매모호하여 그간 논란이 되어 왔다.

이와 관련하여 EU의 정보보호 작업반은 2014. 4. “개인정보보호지침의 제7조상의 정보관리자의 정당한 이익 개념에 대한 06/2014 의견(Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC)[32]"에서 대규모의 개인정보를 정보주체에 대한 공지가 없거나, 또는 정보주체가 예상할 수 없는 범위 내에서 이용하는 것은 정당한 이익으로 해석될 수 없으며, 정당한 이익에 해당한다 하더라도 추가적으로 정보주체의 이익과 이익형량을 해야 한다는 의견을 제시하면서 구체적인 이익형량 기준으로 1)정보이용자의 정당한 이익에 대한 평가, 2) 정보주체에 대한 영향, 3) 잠정적 균형, 4) 정보주체에 대한 적합하지 않은 영향을 방지하기 위한 정보 이용자에 의해 제공되는 추가적이 안정장치 유무 등을 제시한 바 있다. 즉, 위 제7조 제(f)항의 해석을 엄격하게 해야 한다는 의견을 채택한 것이다.

이러한 경향은 최근 유럽사법재판소의 온라인상 잊힐 권리 판결(Case C-131/12 Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzalez)에서도 드러난 바 있다. 유럽사법재판소는 “검색엔진운용자가 정보처리에 가지는 경제적 이익만으로 정보주체의 권리에 대한 침해가 정당화될 수는 없을 것이다. 그러나 결과목록에서 링크를 제거하는 것이 정보에 따라서는 그 정보에의 접근에 관심이 있을 수 있는 인터넷 이용자들의 정당한 이익에 영향을 줄 수 있으므로, 위 이익과 유럽기본권헌정 제7조와 제8조 하의 기본권들(특히 프라이버시와 개인정보를 보호받을 권리)사이의 적절한 균형을 찾아야 한다. 일반적으로 정보주체의 권리가 인터넷 이용자들의 이익보다 우선되는 것은 사실이지만, 적절한 균형은 구체적인 사건들에서 관련 정보의 성격, 정보주체의 사생활에 대한 민감성, (정보주체가 공적 영역에서 담당하고 있는 역할에 따라 달라지는) 당해 정보에의 접근에 공중이 갖는 이익에 따라 결정될 것”[33]이라고 판단한 바 있다.

---

32) http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf

33) 이 판결의 번역은, 헌법재판소 헌법재판연구소에서 뉴스레터로 제공한 2014. 6. 세계헌법재판동향 중 유럽사법재판소 온라인상 잊힐 권리에 관한 유럽사법재판소의 판결(2014. 5. 13.) 제7면을 참조

(3) 개인정보 처리 거부권과 고지의무

위 지침 제14조 제1항은, 제7조 (e), (f)항이 적용되는 경우 정보주체의 특정한 상황과 관련하여 명백하게(compelling) 정당한 이익이 있는 경우 언제라도 자기와 관련된 정보처리를 거부할 권리를 보장하고 있으며, 제14조 제2항은 다이렉트 마케팅 목적으로 사용할 것이 예상되는 개인정보처리를 거절할 권리, 또는 개인정보가 최초로 제3자에게 공개되거나 다이렉트 마케팅 목적을 위하여 이용되기 전에 고지받을 권리, 그리고 그러한 공개나 이용을 비용부담없이 거부할 권리가 명백하게 주어질 권리들을 고지받을 권리를 모두 함께 보장하고 있다.

(4) 프로파일링 거부권

EU 위 지침 제20조에 따르면, 프로파일링을 거부할 권리 눈에 띄게 알려야 한다는 점이 규정되어 있다. 또한, 정보주체에게 법적 효과가 발생하거나, 정보주체의 이익이나 권리 등에 중대한 영향을 미칠 수 있는 조치와 관련되는 프로파일링의 경우에는 특정 요건을 규정하고 있으며, 허용되지 않는 프로파일링도 함께 규정하고 있다.

(5) 소결어

EU의 개인정보보호지침은, 일반적으로 공개된 개인정보를 별도로 규제하기 보다는 지침 제7조 제(f)항에 따라 정보관리자에게 정당한 이익이 있고, 그 이익이 개인정보주체의 기본권과 권리를 침해하지 아니하는 한 범위 내에서 허용될 수 있다. 물론 그 처리가 허용되더라도 지침 제14조에 따라 거부권과 고지의무가 별도로 부여되고 있으며, 제20조에 따라 프로파일링에 대하여는 별도의 제한이 존재한다. 이 지침 제7조 제(f)항의 정당한 이익의 범위는 오늘날 빅데이터 시대에 점점 애매모호해지고 있다. 이와 관련하여 2014. 6.발간된 EU 작업반 의견서에서는 대용량 정보처리가 아무 조건없이 허용되지 않음을 명시하고 있다.

2. 캐나다의 규제

캐나다는 일찍부터 강력한 내용의 개인정보보호법제를 구축 · 운용하여 왔고, 특히 개인정보보호를 위한 독립적인 전담기구를 두고 있을 뿐만 아니라 세계 최초로 정보공개와 개인정보보호를 하나의 법률에 동시에 규정하는 입법례를 택하여 비교법적 고찰의 필요가 있다.[34] 캐나다는 일반적으로 공개된 개인정보에 대하여 EU와는 다른 체계의 입법을 하여 이를 규제하고 있다.

34) 김명식, “캐나다의 개인정보 보호체계에 관한 연구”, 『미국헌법연구』 제23권 제3호, 2012. 12. p.1

가. 개인정보의 정의

캐나다의 개인정보보호 및 전자문서법(PIPEDA, Personal Information Protection and Electronic Documents Act) 제2조 제1항에 따르면 개인정보는 식별가능한 개인에 대한 정보를 의미한다고 규정되어 있는바, 이에는 일반적으로 공개된 개인정보도 포함되는 것으로 해석된다.

나. 일반적으로 공개된 개인정보의 처리 규정

캐나다의 개인정보보호 및 전자문서법 제7조 제1항은 정보주체의 동의나 인식없이 개인정보를 처리할 수 있는 근거규정을 두고 있다. 이에 따르면, 정보주체의 인식이나 동의가 없더라도, (a) 개인정보의 수집이 명백히(clearly) 정보주체의 이익이고, 동의가 시의적절한 방법으로 얻을 수 없는 경우, (b) 정보주체의 인식이나 동의하의 수집이 정보의 정확성과 가용성을 훼손할 것이 예상되는 것이 합리적이고, 그 수집이 협정의 위배, 캐나다법이나 주법의 위반인 경우, (c) 그 정보수집이 오로지 언론, 예술, 문화적 목적인 경우, (d) 정보가 공개적으로 이용가능(publicly available)[35]하며, 법률에 의하여 정해진 경우에 그 처리가 가능한 것으로 규정된다. (제7조 제1항)

캐나다의 개인정보보호 및 전자문서법의 위 제7조 제1항 중 독특한 규정은 (d)의 정보가 공개적으로 이용가능한 경우를 정보주체의 인식이나 동의가 없더라도 수집할 수 있는 조항으로, 캐나다는 이 조항의 적용을 위하여 2000. 12. 13. “공개적으로 이용가능한 정보를 특정하는 규정(Regulations Specifying Publicly Available Information, SOR/2001-7”을 제정하였는데위 규정 제1항 제(e)항에서는 책, 잡지, 신문을 정보를 공개적으로 이용가능한 소스로 적시하고 있다.

이와 관련하여 캐나다의 개인정보보호 및 전자문서법 사례중에 빅데이터와 관련된 개인정보 활용과 관련하여 의미있는 결정이 있었다. 캐나다 개인정보보호위원회는 웹에 게시된 비즈니스 이메일주소(business contact email address)라 할지라도, ① 이는 캐나다의 개인정보보호 및 전자문서법이 정의하고 있는 개인정보이며, ② 언제나 공개적으로 이용가능한 정보로 볼 수 없다라고 판단하였다. 특히 정보주체는 연락주소로 공개하였을 뿐이므로 각종 스팸에 시달리는 것을 예상하지 않았을 것이라는 점도 판단의 근거가 되기도 하였다. 이때 캐나다 개인정보보호위원회는 웹에 게시한 이메일이 정보주체가 편집자(editor)로서 게시한 것과 관련되는 경우에는 공개적으로 이용가능한 개인정보가 될 수 있지만, 웹에 있는 이메일주소라는 사실만으로 공개적으로 이용

35) 공개적으로 이용가능한 정보의 경우 개인정보주체로부터의 수집의무를 면제시켜주는 법제로는 오스트레일리아, 뉴질랜드의 경우에도 유사한 취지의 규정을 두고 있다.
http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-17-2003-privacy-and-personal-information-that-is-publicly-available
https://privacy.org.nz/glossary/#publicly

가능한 정보가 되는 것은 아니라고 판단하였다. 또한 위 사안의 경우에는 개인들로부터 동의를 받아야 하는 비즈니스 이메일 주소를 동의없이 수집한 자로부터 구입하였다 하더라도 동의의무가 면제되는 것이 아니라고까지 판단하였다.[36)]
https://www.priv.gc.ca/cf-dc/2009/2009_013_0602_e.asp

다. 소결어

캐나다의 개인정보규제에 의하더라도, 일반적으로 공개된 개인정보는 개인정보보호법의 규제내에서 처리되어야 한다. 다만 캐나다는 공개적으로 이용가능한 소스에 대하여는 예외규정을 두고 있으나 그 범위를 제한적으로 해 석해 왔다.

3. 미국 캘리포니아 법

미국의 경우 민간분야에서 통일된 개인정보보호법 자체가 없다. 물론 공공분야에 있어서는 엄격한 개인정보보호법이 있으나, 민간에서는 일부 영역에 한정하여 개인정보보호법이 존재할 뿐이다.

이와 관련하여 온라인 상의 프라이버시 보호법이 캘리포니아에서 2003년에 제정되었는데, 이에 따르면 캘리포니아 주에 거주하는 개인정보를 웹사이트를 통하여 수집하는 상업성 웹사이트 또는 온라인 서비스 운영자들에게 프라이버시 정책에 대한 구체적인 고지를 할 것이 의무화되어 있다.

미국의 경우에는 개인정보 보호법 자체가 발전되지 못하였고 이에 따라 EU나 캐나다 등에서 나타난 것과 같은 민간에서 통일적으로 규정할 법률자체가 존재하지 않는 상황이다. 그럼에도 불구하고 위 미국의 캘리포니아 프라이버시 보호법은, "웹사이트상의 개인정보" 역시 보호받아야 하는 개인정보라는 전제가 있다라는 점을 시사점으로 확인할 수 있다.

4. UN 결의안

2014. 9. 23. 제69차 유엔총회에서 유엔 반테러와 인권보장에 관한 특별보고관의 보고서에 따르면, 각 국가 대량 감시 프로그램이 온라인상의 프라이버시를 실질적으로 완전히 말살해 버렸다는 사실을 똑바로 직시할 필요가 있으며, 사생활에 간섭하는 수단들은 합법적인 목표를 추구하고, 공개적으로 접근가능하며, 엄격하게 국내법에 의하여 허가를 받아야 하며 비례의 원칙에 따라 불가피한 경우에 허용되어야 함을 보고한 바 있다.

---

36) PIPEDA Case Summary #2009-013 https://www.priv.gc.ca/cf-dc/2009/2009_013_0602_e.asp

5. 소결어

일반적으로 공개된 개인정보에 대하여 개인정보보호의 법체계를 뛰어넘는 입법례는 쉽게 찾아보기 힘들다. 과거 프라이버시 보호법제에서 쉽게 예상하지 못했던 빅데이터 기술들은 오늘날 사생활의 범위를 축소시켜가고 있다. EU의 경우 이러한 사정하에서 기존의 EU 개인정보보호지침 만으로는 개인정보보호가 쉽지 않다는 점을 고려하여 최근 일반개인정보보호법의 제정작업을 진행하고 있다.

Ⅲ. 국내에서의 공개된 개인정보의 논란

국내에서는 방송통신위원회에 의하여 추진되고 있는 "빅데이터 개인정보보호 가이드라인"이 공개된 개인정보에 대한 법적 논란을 제기하였고, 이후 원세훈 판결 등 다양한 사건들에서 공개된 개인정보의 처리에 대한 해석들이 법원 판결을 통해 드러난 바 있다.

1. 빅데이터 개인정보보호 가이드라인

가. 정부의 공약사업으로 추진

일반적으로 공개된 개인정보의 활용과 관련되어 가장 두드러지게 드러난 사건은 작년 연말부터 추진된 빅데이터 개인정보보호 가이드라인안이라 할 것이다. 미래창조부는 2013. 12. 11. 빅데이터산업육성을 창조경제 및 정부 3.0의 핵심동력이라고 설명하면서 이의 법과 관련 제도의 정비에 대한 중요 추진계획으로 제시한 바 있다.[37] 이후 방송통신위원회는 2013. 12. 18. "공개된 개인정보 또는 이용내역 정보 등을 전자적으로 설정된 체계에 의해 조합, 분석 또는 처리하여 새로운 정보를 생성함에 있어서 이용자의 프라이버시 등을 보호하고 안전한 이용환경을 조성하는 것을 목적"으로 하는 "빅데이터 개인정보보호 가이드라인"을 발표하였다. 이 가이드라인의 내용에 따르면 **공개된 개인정보**에 한하여 개인정보의 수집, 이용내역정보 수집, 새로운 개인정보 생성, 조합 · 분석· 처리, 이용, 제3자 제공 등의 처리과정에 대하여 개인정보보호법의 적용을 우회하여 개인정보주체의 동의없이 허용할 수 있도록 하고 있었다.[38]

나. 개인정보보호위원회의 결정

위 "빅데이터개인정보보호가이드라인"에 대하여 경실련, 진보네트워크, 함께하는 시

37) 미래창조과학부,"빅데이터 산업 발전 전략 보도자료", 2013. 12. 11. http://www.msip.go.kr/www/brd/m_211/view.do?seq=1119

38) 미래창조과학부, "빅데이터 페어 2013 보도자료", 2013. 12. 18. \ http://www.msip.go.kr/www/brd/m_211/view.do?seq=1163&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=68

민행동은 개인정보보호법위반의 우려가 있다는 이유로 위 가이드라인을 개인정보보호위원회에 신고하였다. 개인정보보호위원회는 “빅데이터개인정보가이드라인”이 개인정보보호법 제15조 등의 위반임을 문제삼아 방송통신위원회에 개인정보 보호 관련 법률의 내용과 체계에 부합하도록 재검토할 것을 방송통신위원회 위원장에게 권고하는 결정을 하였다.

현행 개인정보 보호법 및 정보통신망법은 ‘공개된 개인정보’나 ‘이용내역정보’를 달리 취급하여 규정하고 있지 않으므로 정보주체의 자기결정권을 보장해 주기 위하여 모든 개인정보 수집 시 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에도 그 불이익의 내용을 정보주체에게 고지하고 정보주체로부터 명시적인 동의를 받도록 하며, 다만 다른 법률에 특별한 규정이 있는 등의 몇 가지 예외사유에 한정하여 동의없는 수집을 허용하고 그 수집 목적의 범위 내에서만 수집된 개인정보를 이용할 수 있도록 하는 규정들(개인정보 보호법 제15조, 정보통신망법 제22조, 제24조 등)은 ‘공개된 개인정보’ 및 ‘이용내역정보’에도 그래도 적용된다 할 것이다. 그럼에도 가이드라인(수정안)은 ‘공개된 개인정보의 경우’의 경우 정보주체의 동의가 없어도 이를 수집할 수 있도록 허용하고 있는데 제한없이 일반 공중에게 공개되었다 하여 개인정보 보호법이나 정보통신망법의 규제를 받지 않는다거나 구체적 사정을 고려함이 없이 해당되는 모든 정보주체가 그 수집에 필요한 동의를 한 것으로 해석하거나 간주할 수는 없다.

표1 빅데이터 개인정보보호 가이드라인에 대한 개인정보보호위원회의 결정

다. 수정된 빅데이터 개인정보 보호 가이드라인의 제안

개인정보보호위원회로부터 위와 같은 결정이 나온 이후, 방송통신위원회 최성준 위원장은 2018. 10. 14. 미래창조과학방송통신위원회 국정감사에서 “법에 명백히 위반되는 것은 만들 수 없다. 그러나 법해석상 여지가 있는 것은 가이드라인 형식으로 추진할 수 있다”라고 답변하여 빅데이터와 관련된 법 체계의 정비를 가이드라인 형식으로 추진할 의사를 표시하였고[39], 이후 비식별화 조치를 강화하는 조건으로 2014. 11. 20. 정보보호 가이드라인(안)을 공개한 바 있다.

39)미디어스, “최성준 빅데이터 가이드라인 좌초 아냐 … 추진할 것”, 2014. 10. 15.

라. 비식별화와 관련된 쟁점들

과연 비식별화조치를 취하면, 개인정보보호법의 적용이 배제되는 것일까. 사실 이 부분은 명확하지 않은 부분들이 존재한다. 우선, "비식별화 조치"의 범위를 어떻게 법규상 정의할 것인지가 명확하지 않다. 둘째, "비식별화 조치"를 시킨 이후의 개인정보가 다시 재식별화될 가능성이 존재할 경우에 대한 법적 처리에 대하여도 위 가이드라인은 다시 비식별화하면 된다고만 정리하고 있을 뿐이다.[40] 이 논쟁은 현재 위 가이드라인의 내용이 모두 공개되지 않은 상황이라 향후 좀 더 조문들이 구체화되면 다시 재연될 것으로 예상된다.

2. 서울중앙지방법원 2014. 9. 11. 선고 2013고합577, 1060(병합) 공직선거법위반, 국가정보원법위반 판결 (이하 "원세훈 판결")

가. 원세훈 판결의 내용

서울중앙지방법원에서는 국정원장이었던 원세훈에 대한 형사판결에서 일반적으로 공개된 개인정보에 관련된 쟁점에 대하여 판단을 하였다.

원세훈 판결은, 헌법재판소 2005. 5. 26. 99헌마513 사건[41]에서 공개된 개인정보라 하더라도 자기결정통제권의 대상이 되고 있음을 판시하였다는 점을 근거로 공개된 개인정보의 경우 개인정보보호법이 적용됨을 전제로 "개인정보처리자가 개인주체 이외로부터 개인정보를 수집하여 처리하는 경우에는 개인정보의 수집 및 이용에 관한 개인정보 보호법 제15조보다 위 조항(개인정보 보호법 제20조)이 우선 적용되는 것으로 해석함이 타당 … (중략) … 빅데이터업체가 트위터 정보를 수집한 것은 개인정보보호법 제20조 제1항에 해당하여 해당정보주체의 개별적 동의가 없다고 하더라도 그러한 사정만으로 개인정보 보호법에 위반한 위법행위로 평가할 수 없다"라고 판단한 바 있다(서울중앙지방법원 2014. 9. 11. 선고 2013고합577, 1060(병합) 공직선거법위반, 국가정보원법위반 판결).

---

40) 2014. 11. 20.자 빅데이터 개인정보보호 가이드라인에 대하여 온라인에 공개되어 있지 않고, 정보공개청구를 하였으나 우편으로 보내주겠다는 답변을 받아 현재 위 가이드라인의 내용은 정확히 확인할 수 없는 상황이다.

41) 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 가티 개인의 인격주체성을 특정짓는 사항으로서 그 개인의 동일성을 식별하 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사의 영역에 속하는 정보에 국한되지 않고 공적생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 자기정보결정권에 대한 제한에 해당한다 (헌재 2005. 5. 26. 선고 99헌마513 등, 2005. 7. 21. 선고 2003헌마282·425(병합), 2011. 12. 29. 선고 2010헌마293, 2014. 7. 24. 선고 2013헌마423·426 등 다수)

개인정보보호법 제20조 제1항은 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 개인정보의 수집 출처, 개인정보의 처리 목적, 개인정보의 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알려야 한다고 정하고 있는바, 위 규정은 이 사건과 같이 개인정보처리자가 개인정보를 공개된 출처로부터 수집하거나 본인이 아닌 제3자로부터 수집하여 처리하는 경우 해당 개인정보를 수집하기 이전에 정보주체로부터 개별적으로 동의를 받거나 수집 사실을 미리 통지하는 것이 불가능한 경우가 많기 때문에 사후적으로 정보주체에게 자신의 개인정보처리를 정지할 수 있는 권한을 부여하기 위함에 그 입법취지가 있다고 봄이 타당하고, 따라서 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 경우에는 개인정보의 수집 및 이용에 관한 개인정보보호법 제15조보다 위 조항이 우선 적용되는 것으로 해석함이 타당하다.

서울중앙지방법원 판결문 판결 이유 제59면

나. 개인정보보호법 제15조와 제20조간의 관계

원세훈 판결은 제3자로부터 수집하여 처리하는 경우에는 개인정보보호법 제20조가 제15조에 우선하여 해석되는 것처럼 해석하고 있다. 하지만 이 해석은 다음과 같은 점에서 타당하지 않다.

우선, 개인정보 보호법 제15조(개인정보의 수집· 이용)에서 정한 정보주체의 동의 원칙의 예외 규정은 같은 법 제18조 제2항(개인정보의 목적 외 이용 · 제공 제한)의 규정에 따라야 하므로, 같은 법 제18조 제2항의 규정에 해당하지 아니하는 한, 공개된 개인정보라 하더라도 개인정보 보호법 제15조의 적용에 따라야 할 것이다.

둘째, 개인정보 보호법 제20조(정보주체이외로부터 수집한 개인정보의 수집 출처등 고지)는, 개인정보처리자가 정보주체로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 하는 고지의무만을 규정하고 있을 뿐, 개인정보처리자의 수집권한과 관련된 요건을 규정하고 있는 규정이 아니다. 이와 관련하여 비슷한 입법체계를 가지고 있는 EU 개인정보보호지침에서도 앞에서 본 것과 같이 제7조에서 동의를 받지 않고 처리할 수 있는 예외조항을 규정한 뒤, 그 뒤 별개의 추가 요건을 제14조, 제20조에서 하고 있음을 하고 있다는 점에서도 위 원세훈 판결의 해석은 타당하지 않다 할 것이다.

이 점에 대하여 인물정보 사건에서는 아래에서 보는 바와 같이 일반적으로 공개된 개인정보의 처리에 대하여 개인정보 보호법 제20조가 제15조에 우선하는 것이 아님을 설명한 바 있다.

3. 서울중앙지방법원 2014. 11. 4. 선고 2013나49885 부당이득금반환 판결 (이하 “인물정보 사건”)

가. 인물정보 사건의 판결 내용 및 쟁점

인물정보 사건은, 유료로 인물정보를 제공하는 언론사에 대하여 개인정보주체가 개인정보자기결정권침해를 원인으로 손해배상소송을 구한 사건인데, 이 사건에서는 일반적으로 공개된 개인정보의 개인정보주체의 동의없이 처리가능성에 대한 법해석이 논란이 되었다.

이 사건에서 법원은 일반적으로 공개된 개인정보의 동의없는 처리가 가능한 경우에 대하여 개인정보 보호법 제15조 제1항 등에 의하여 동의가 묵시적으로 있었다고 인정되는 해석할 수 있는 경우에 한정하여 인정하고, 개인정보 보호법 제20조가 제15조에 우선하지 않는다고 판단하였다.

> 2. 피고 1에 대한 판단
>
> … 원고가 공적 존재인 대학교수인 점, … 위 화면에 게재된 원고의 개인정보는 공개된 매체인 OO대학교 홈페이지에 이미 공개되어 있는 원고의 개인정보 중에서도 가장 기본이 되는 직업적 정보인 점 등에 비추어 피고 1이 위와 같은 정도로 원고의 개인정보를 인터넷에 노출시킨 것은 원고의 개인정보 보호법 제15조 제1항 제1호 및 제17조 제1항 제1호 소정의 각 동의가 묵시적으로 있었다고 인정되는 범위 내의 것으로 봄이 타당하므로…
>
> 3. 피고 5에 대한 판단
>
> … 살피건대, 개인정보 보호법의 전체 체계 내에서 제20조가 어떤 의미를 갖고 있는지가 다소 불분명하기는 하나 (그 구체적인 입법이유를 확인할 만한 자료가 없어 보인다), ① 개인정보 보호법 제17조가 개인정보의 제공 요건을 규정하면서 그 대상을 ‘정보주체의 개인정보’라고 표현하고 있을 뿐 ‘정보주체로부터 직접 수집한 개인정보’라고 표현하고 있지도 아니하고, 공개된 개인정보와 그러하지 아니한 개인정보를 구분하고 있지도 아니한 점, ② 개인정보의 보호와 관련하여 현실적으로 공개된 개인정보를 어떻게 보호할 것인가가 주로 문제되는데, 개인정보 보호법 제20조의 취지를 피고 5의 위 주장과 같이 해석할 경우, 개인정보 보호법 전체의 입법취지가 몰각될 우려가 있는 점 등에 비추어, 개인정보 보호법 제20조 제1항은 개인정보처리자가 공개된 개인정보를 그 공개된 자료의 성질이나 공개 당시의 상황에 비추어 정보주체의 동의 의

사가 있었다고 인정되는 범위 내에서 비영리 목적으로 이를 수집.이용.제공하는 등의 처리를 할 수 있고, 이러한 경우 정보주체의 사후적인 통제권이 인정된다는 취지의 규정으로 해석함이 타당한 것으로 보이고, 공개된 개인정보의 경우 정보주체의 사후적인 통제권만 인정되고, 그 사후적인 통제권이 행사되기 이전에는 이를 일률적으로 제한 없이 수집.이용.제공하는 등의 처리를 할 수 있다는 취지의 규정으로 해석함은 적절하지 않은 것

나. 동의 조항의 해석

인물정보 사건은 개인정보 보호법 제15조 및 제17조의 동의의 개념을 묵시적으로 해석하였다. 그러나 이러한 개인정보보호법에 있어서의 동의는 동의여부가 명확하게 확인할 수 있는 형태로 이루어지는 것을 원칙으로 하고 있다는 점에서 묵시적인 동의를 인정하는 것은 개인정보보호법상의 동의의 원칙을 우회할 수 있는 위험성이 존재한다. 2011. 6. 13. 채택된 EU 데이터보호 작업반의 동의 정의에 대한 의견(Opinion 15/2011 on the definition of consent)에 따르면 동의는 명확하게 특정하게 이루어져야 하기 때문에 묵시적으로 이루어지는 것으로 해석되기는 어렵다.

일반적으로 공개된 개인정보의 처리와 관련하여서는 EU 개인정보 지침 제7조 제f항과 대응되는 개인정보 보호법 제15조 제1항 제6호에 따라 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우, 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한하여 허용하는 경우로 법해석하는 것이 타당하였을 것으로 판단된다.

4. 소결어

일반적으로 공개된 개인정보의 개인정보 보호법상의 법해석을 정리하면 다음과 같이 정리할 수 있을 것이다.

가. 일반적으로 공개된 개인정보의 경우에도 개인정보 보호법 제2조 제1호의 개인정보의 정의에 포함된다.
나. 일반적으로 공개된 개인정보의 활용은 개인정보 보호법 제15조 제1항 제6호에 따라 판단할 수 있다.
다. 개인정보 보호법 제20조는 개인정보 보호법 제15조에 우선하는 규정이 아니라, 개인정보 보호법 제15조와 함께 적용되는 규정이다.

프로파일링의 제한 / 금지 / 거부

정 혜 승

무엇이 문제인가?

왜곡

감시 (국가 or 사인)

편견의 조장

상업적 사용(남용)

프로파일링의 제한 / 금지

금지와 제한은 연결되어 있음

EU – 프로파일링의 절대적 금지 범위 설정

"Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited.

프로파일링의 제한 / 금지

제한이 과연 가능한가?

- 기술적이며 내밀한 문제

왜곡가능성!!

- 알고리즘 모름
- 투입정보, 변수에 따른 변화
- 오류발생 가능성

(사례) 심평원의 데이터마이닝 과정

프로파일링의 제한 / 금지

1. 국가에 의한 감시

- (사례)
- 미국 소셜 네트워크를 통한 범죄집단 감시
- 미국 국방부의 인적자원 관리를 위한 데이터마이닝
- 싱가포르 국가위험관리시스템
- 건강보험 부당청구 / 사무장병원 적발
- 연금 부당청구 적발
- 국민연금 지역가입자 신고소득 적정성 점검

법적 근거가 부족함

국가의 감시수단이 될 수 있는 분야는 개별법에 근거를 명확히

프로파일링 결과가 유일한 처분근거 / 최종판단이 되어서는 안됨

경향성 파악, 수사 및 조사의 단서, 감사의 단서로만 사용

프로파일링 결과 증거사용 금지

프로파일링의 제한 / 금지

2. 사인에 의한 감시

(사례) 기업의 개인에 대한 정보수집/분석 결과의 활용

동의가 있으면 가능한가?

침익적 사용 가능?

프로파일링의 제한 / 금지

3. 편견의 조장

(사례) 카드사의 맛집 순위 발표

정보처리의 방법

- 단순한 비교 및 순위 매기기 -> 객관적 확인이 가능함
- 분류(classify) / 군집화(clustering) / 연관짓기(association)

프로파일링된 정보 공표의 금지

프로파일링의 제한 / 금지

4. 상업적 사용(남용)

가장 많이 활용되는 예

왜곡의 가능성은 가장 낮음

프로파일링에 대한 명확한 동의를 얻어 사용범위 넓히는 방안?

프로파일링의 조작 -> 제재가능성?

공개된 정보 / 공공정보 공개

제공자들은 동의했을까?

(사례) 심평원의 공개정보

- 질병별 환자수 / 전국 과별 처방약 순위

법률의 규정이 있는가?

수집범위를 넘어 프로파일링한 경우 손해배상 청구?

빅데이터 개인정보보호 가이드라인과 비식별화 가이드라인 비판

이은우(법무법인 지향)

1. 빅데이터 개인정보보호 가이드라인이 불러올 여파

가. 빅데이터 개인정보보호 가이드라인은 두 마리 토끼를 잡을 묘안인가?

- 방통위는 2014년 12월 23일 '빅데이터 개인정보보호 가이드라인'(이하 '가이드라인')을 발표하였다.
- 보도자료에서 방통위는 이를 "개인정보의 오·남용을 방지하면서, 빅데이터 산업의 활성화라는 두 마리 토끼를 잡을 묘안"이라고 하였다.
- 방통위는 가이드라인을 "사업자 등에게 새로운 의무나 제한을 가하지 않도록 하되, 현행 법령 테두리 안에서 개인정보 보호를 위해 사업자가 지켜야 할 기술적·절차적 사항을 구체적으로 규정한 것"이라고 한다.

나. 가이드라인은 개인정보보호법을 위반하는 내용을 담고 있다

- 방통위는 가이드라인의 내용을 다음과 같이 설명한다.
- "빅데이터 처리 과정에서 수집된 데이터에 개인정보가 포함된 경우, 이를 다른 정보로 대체하거나 다른 정보와 결합하여도 특정 개인을 식별하기 어렵도록 하는 '비식별화' 조치가 선행된다면 수집·활용이 가능하도록 했다. 사업자들의 규제 불확실성을 최소화하기 위해 현행 법령 내에서 공개된 정보 등을 합법적으로 수집·활용할 수 있는 구체적인 기준을 제시한 것이다."
- "데이터의 수집 단계에서 개인정보를 비식별화 하였다 하더라도 조합·분석 단계에서 다른 정보와 결합하여 재식별화 될 수 있는 가능성이 있는 경우 반드시 이를 즉시 파기하거나 추가적인 비식별화 조치를 취하도록 명시하였다."
- 이처럼 가이드라인의 핵심은 비식별화인데, 가이드라인의 비식별화는 동의를 받지 않아도 될 익명화 처리와는 거리가 멀고, 현행 개인정보보호법에 위반되는 내용들이 포함되어 있다.

2. 가이드라인의 용어 사용 문제

가. 법령은 표준적인 용어를 사용해야 한다

- 법령에서 용어의 정의를 두는 이유는 불명확하거나 여러 뜻으로 사용되는 것을 명확하게 하기 위함이다..[1]

---

[1] "용어의 의미는 일반적으로 사전에 설명된 내용대로 사용되거나 사회통념에 따라 정해지는 것이지만 하나의 용어가 여러 뜻으로 쓰이는 경우가 많다. 이런 경우에 그 법령에서 어떤 의미로 그 용어를 사용하는가를 명확하게 해 둠으로써 법령의 해석과 적용상의 혼란을 막을 수 있다. 이와 같이 정의 규정은 법령해석상의 논란을 예방하고, 법령의 집행 과정에서 발생할 수 있는 분쟁을 방지할 뿐만 아니라, 여러 조문에서 자주 사용되는 용어를 미리 하나의 조문에서 설명해 줌으

- 정의에 사용되는 용어는 법령 상호간 통일시켜야 한다. 사회통념상 확립된 의미와 동떨어진 용어의 정의는 법령의 의미를 알기 어렵게 할 우려가 있다.[2]

나. 가이드라인은 잘못된 용어를 사용하고 있다

(1) 비식별화 – 첫 번째 숨겨진 발톱

- 가이드라인의 비식별화의 정의
  - "비식별화"란 데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별할 수 없도록 하는 조치를 말한다.
- '비식별화 처리'를 하면 '개인정보보호법'의 '개인정보'가 아닌 것이 되어, '개인정보보호법'의 적용이 배제되는가?
  - 만약 그렇지 않다면 '가이드라인'은 위법한 행위를 적법하다고 호도하여 허용하는 것이다.
  - 가이드라인에서 정의한 '비식별화'는 진정으로 비식별화된 것인가?
  - 비식별화라는 용어는 잘못 사용된 용어이다.
  - 개인정보보호법이 적용되지 않으려면 비식별화가 아니라 익명화 처리가 되어 개인을 식별할 가능성이 없어야 한다.

(2) 정보처리 시스템 – 두 번째 숨겨진 발톱

- 가이드라인의 정보처리 시스템의 정의
  - "정보처리 시스템"이란 공개된 개인정보 또는 이용내역정보 등을 전자적으로 설정된 체계에 의해 조합·분석 등 처리하여 새로운 정보를 생성하는 시스템을 말한다.
- 가이드라인의 정보처리시스템은 프로파일링의 숨겨진 표현
  - '프로파일링'은 매우 위험스러운 개인정보의 처리로, 세계적으로 추가적인 보호조치가 필요하다고 보고 있다.

3. 비식별화(de-identification), 익명화(anonymization), 가명화(pseudonymization)

로써 법령문을 간결하게 표현할 수 있게 한다."(법제처, '법령입안심사기준')

[2] 정의 규정에서는 「대한민국 헌법」이나「민법」과 「형법」 등 기본법에서 사용하는 용어와 표현을 존중하여 같은 용어는 가능하면 뜻이 같도록 표현하는 것이 바람직하다. 법령 상호간의 용어를 통일시킴으로써 법 규정의 내용에 대한 이해를 더 쉽게 할 수 있고 법령의 집행 과정에서도 법 규정을 더 명확하게 해석할 수 있기 때문이다. 사회통념상 확립된 의미와는 동떨어진 용어 정의는 법령의 의미를 알기 어렵게 할 우려가 있으므로, 가능하면 일반적으로 사용되는 용어의 용법에 맞게 용어 정의를 해야 한다. 법령 가운데 어떤 용어를 정의할 필요가 있는가에 관해서는 그 용어가 지니는 의미의 다양성과 그 용어가 법령상 차지하는 비중과 법적 효력상의 중요성 등에 따라 합리적으로 판단해야 할 것이다. 그리고 용어 정의가 없는 경우에는 건전한 상식에 따라 판단해야 할 것이다.

가. 비식별화(de-identification), 익명화(anonymization)

- 두 가지 개념 모두 재식별화의 가능성이 있음.
- 비식별화라는 개념보다는 익명화라는 개념을 사용함.
- 유럽의 경우도 비식별화라는 용어를 사용하지 않고, 익명화라는 용어를 사용함.
- 독일에서는 비개인화(depersonalization)[3]이라는 용어를 사용함.

나. 익명화에 대한 별도의 규정을 둘 것인가?

- 익명화된 정보(anomized data)에 대한 정의를 별도로 둘 것인가? 개인정보가 다시 개인이 식별될 가능성이 없도록 익명화되었다면 해당 정보는 개인정보로 볼 수 없는가?
- 유럽연합 Directive 95/46 EC의 태도
  - 지침의 규정에는 포함시키지 않고, Recital 26.[4]에 익명화된 데이터(data rendered anonymous)에 대한 표현을 둠. 개인이 더 이상('no longer possible') 식별될 가능성이 없다면. 개인정보로 보지 않는다고 함.

다. 익명화의 정의

- 익명화에 대한 표준적 정의는 없음. 몇 가지 시도는 있음. 예를 들어 ISO의 정의.
  - 익명화 : 개인 정보(개인식별 가능정보)가 정보주체가 더 이상 직접 또는 간접적으로 정보처리자 또는 제3자와의 협력으로 개인을 식별할 수 없도록 회복 불가능하게 변경하는 절차(ISO 29100, 2011)[5]

---

[3] 그런데 이 용어는 비현실적인 느낌이나 자기자신 또는 자기 신체상에 대한 이상한 느낌 등을 느끼는 증상으로 이인증이라고부른다. 이인증은 현기, 불안, 광기에 대한 공포와 비현실감 등이 흔히 동반된다고 한다.

[4] "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;".

[5] "Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party"

- 유럽연합의 국가들 중에서도 일부 국가에서만 익명화에 대해 규정함.
  - 독일 연방 데이터 보호법[6] Section 3 (7) "Depersonalization" means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.
  - 슬로베니아. 스페인[7] 등 일부 국가
- 익명화는 흔히 재식별화가 불가능하게 처리하는 것. 또는 재식별화의 실질적 가능성이 없는 것을 의미함.
- 유럽연합 Working Party 29는 재식별화(re-identification)의 가능성 때문에 익명성(anonymity)이나 익명 정보(anonymous data)라는 표현보다 익명화 기술(anonymisation technique)이라고 기술함.

라. 생명윤리 및 안전에 관한 법률

- 생명윤리 및 안전에 관한 법률은 익명화에 대한 정의가 있는데, 개인정보보호에 부적절함.
- "익명화"(匿名化)란 개인식별정보를 영구적으로 삭제하거나, 개인식별정보의 전부 또는 일부를 해당 기관의 고유식별기호로 대체하는 것을 말한다고 정의함(제2조).
- 생명윤리 및 안전에 관한 법률 제18조는 '인간대상연구자는 연구대상자로부터 개인정보를 제공하는 것에 대하여 서면동의를 받은 경우에는 기관위원회의 심의를 거쳐 개인정보를 제3자에게 제공할 수 있다'고 규정하고, '인간대상연구자가 개인정보를 제3자에게 제공하는 경우에는 익명화하여야 한다. 다만, 연구대상자

---

[6] Section 30 Storage of data in the normal course of business for the purpose of communication in depersonalized form (1) If personal data are stored in the normal course of business in order to communicate them in depersonalized form, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. Such characteristics may be combined with the information only where necessary for storage or scientific purposes. (2) The modification of personal data shall be admissible if 1. there is no reason to assume that the data subject has a legitimate interest in his data being excluded from modification or 2. the data can be taken from generally accessible sources or the controller of the data file would be entitled to publish them, unless the data subject clearly has an overriding legitimate interest in his data being excluded from modification. (3) Personal data shall be erased if their storage is inadmissible. (4) Sections 29, 33 to 35 of this Act shall not apply.

[7] Spanish Data Protection Act, Art. 3(f). "any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person.

가 개인식별정보를 포함하는 것에 동의한 경우에는 그러하지 아니하다.'고 규정함.

- 이 법률의 익명화는 진정한 의미의 익명화로 볼 수 없음.

4. 익명화 기술에 대하여

가. 익명화 기술 개요[8]

(1) 익명화 기술은 크게 무작위화(randomization) 방법과 일반화(generalization) 방법이 있다.[9]

- 무작위화 방법에는 잡음 추가 방법, 순열 방법, 차등 정보보호 방법(Differential privacy), 대체, 일반화 방법에는 총계처리(Aggregation)와 K-익명성(K-anonymity) 방법, l-다양성 (l-diversity)/ T-근접성(T-closeness).

(2) 익명화 기술들의 재식별화의 위험

- 익명화 기술들은 재식별화의 가능성이 있다.
- 재식별화의 가능성은 3가지 측면을 고려해야 한다
  - Single out(개별화)[10]
  - Linkability(연결 가능성)[11]
  - Inference(추론 가능성)[12]

---

[8] 유럽연합 29조 작업반, Opinion 05/2014 on Anonymisation Techniques(2014년 4월 10일)

[9] 위 자료 12 페이지

[10] 위 자료 11 페이지, Singling out , which corresponds to the possibility to isolate some or all records which identify an individual in the dataset

[11] 위 자료 11 페이지, Linkability, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability

[12] 위 자료 12 페이지, Inference, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.

	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

(출처 : 유럽연합 29조 작업반, Opinion 05/2014 on Anonymisation Techniques, 24 페이지, 2014년 4월 10일)

나. 가명화[13]

- 가명화는 익명화된 것으로 보기 어렵다.
- 개별화, 연결 가능성, 추론 가능성 모두 남아 있다.

다. 익명화와 재식별화의 가능성

- 재식별화의 가능성이 있으면 익명화된 것으로 볼 수 없다.
- 재식별화이 가능성은 비용, 시간, 기술 등을 고려해야 한다. 기술 발전에 따라 비용이 계속 낮아지는 점, 재식별화를 위해 가용한 정보가 증가한다는 점도 고려해야 한다. 특히 기술의 발전 속도가 매우 빠르기 때문에 현재의 기술 뿐만 아니라, 기술의 발전가능성을 반드시 고려해야 한다.[14]

라. 익명화 조치시 유념해야 할 사항

- 일반적 요소 : 익명화하여 제공하고 잊어 버리는 정책이어서는 안됨. 재식별화의 남은 위험성이 있다면 정보처리자는 1) 새로운 위험을 찾아내고, 재식별화의 잠재적 위험을 지속적으로 재평가한다. 2) 확인되는 위험을 통제할 수 있는지 평가하고, 그에 따라 조정한다. 그리고 3) 위험을 모니터하고 통제한다.[15]
- 기술적 요소[16]

---

[13] 위 자료 20 페이지 ~ 22 페이지

[14] 위 자료 8 페이지

[15] 위 자료 24 페이지. As part of such residual risks, take into account the identification potential of the nonanonymised portion of a dataset (if any), especially when combined with the anonymised portion, plus of possible correlations between attributes (e.g. between geographical location and wealth level data).

[16] 위 자료 25 페이지. Technical elements: - Data controllers should disclose the anonymisation

- 상황적 요소[17]

5. 우리나라 개인정보보호법의 개인정보의 비식별화나 익명화에 대한 태도

가. 우리나라 개인정보보호법은 비식별화 또는 익명화한 정보에 대한 특별규정을 두고 있는가?

- 우리나라 개인정보보호법에 '비식별화' '익명화' 또는 '비식별화한 개인정보'나 '익명화한 개인정보'에 대한 특별한 규정은 없음.
- 예를 들어 독일의 데이터보호법, 유럽연합의 지침은 규정에는 없고, 전문에 있음.

나. 우리나라 개인정보보호법상 비식별화 또는 익명화한 정보는 개인정보로 볼 수 있는가? 개인정보가 아닌가?

---

technique / the mix of techniques being implemented, especially if they plan to release the anonymised dataset. - Obvious (e.g. rare) attributes / quasi-identifiers should be removed from the dataset. - If noise addition techniques are used (in randomization), the noise level added to the records should be determined as a function of the value of an attribute (that is, no out-ofscale noise should be injected), the impact for data subjects of the attributes to be protected, and/or the sparseness of the dataset. - When relying on differential privacy (in randomization), account should be taken of the need to keep track of queries so as to detect privacy-intrusive queries as the intrusiveness of queries is cumulative. - If generalization techniques are implemented, it is fundamental for the data controller not to limit themselves to one generalization criterion even for the same attribute; that is to say, different location granularities or different time intervals should be selected. The selection of the criterion to be applied must be driven by the distribution of the attribute values in the given population. Not all distributions lend themselves to being generalized – i.e., no one-size-fits-all approach can be followed in generalization. Variability within equivalence classes should be ensured; for instance, a specific threshold should be selected depending on the "contextual elements" mentioned above (sample size, etc.) and if that threshold is not reached, then the specific sample should be discarded (or a different generalization criterion should be set).

[17] 위 자료 25 페이지. Contextual elements: - The purposes to be achieved by way of the anonymised dataset should be clearly set out as they play a key role in determining the identification risk. - This goes hand in hand with the consideration of all the relevant contextual elements – e.g., nature of the original data, control mechanisms in place (including security measures to restrict access to the datasets), sample size (quantitative features), availability of public information resources (to be relied upon by the recipients), envisaged release of data to third parties (limited, unlimited e.g. on the Internet, etc.). - Consideration should be given to possible attackers by taking account of the appeal of the data for targeted attacks (again, sensitivity of the information and nature of the data will be key factors in this regard).

- 현재 개인정보보호법제에서 '비식별화'한 개인정보 또는 익명화한 개인정보를 특별히 규정하고 있지 않으므로 개인정보보호법의 정의에 충실해야 함.
- 개인정보보호법, 정통망법은 개인정보를 "살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다"고 정의.
- 이 정의는 유럽연합의 개인정보보호지침의 개인정보의 정의 규정이나, 새로 제안된 GDPR의 개인정보의 정의 규정[18]이나, 각국의 개인정보보호 관련 법률의 개인정보에 대한 정의와 크게 다르지 않음.
- '쉽게'라는 표현이 들어 있는데, 이를 특별히 해석의 기준으로 의미를 두고 있지는 않음.
- 수집, 처리주체는 물론 제3자로부터의 추가 정보를 합하여 개인이 식별될 가능성이 있다면 개인정보로 봄. 단, 비용, 시간, 기술에서 비합리적으로 부당하게 과도한 노력이 필요한 수준이라면 제외함.
- 결국, '다른 정보와 결합하여 특정 개인을 알아볼 수 있다면', 즉, 재식별화(re-identification) 가능하다면 개인정보로 볼 것임.
- 결국 '재식별화'의 가능성 즉, 비식별화나 익명화의 수준에 의하여 개인정보보호법 적용 여부가 결정될 것임.

6. 현행 법제의 해석상 개인정보를 수집한 후 개인을 식별할 수 없게 하여 처리하는 것은 적법한가?

가. 개인정보 수집시의 동의의 원칙

- 현재 개인정보보호법은 개인정보를 수집할 때는 개인정보주체에게 수집항목, 처리목적, 보유기간, 개인정보주체의 권리, 필수정보가 아니면 수집에 동의하지 않아도 된다는 점을 알리도록 규정한다.

[18] (1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
(2) 'personal data' means any information relating to a data subject;

제15조(개인정보의 수집•이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보의 수집•이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

나. 개인정보를 수집한 후 익명화하여 이용하는 것에 대해서는 동의를 받지 않아도 되는가?

사례 1 : 이동통신사에서 개인정보를 수집한 후 그와 같은 개인정보를 해당 개인의 동의를 받지 않고, 익명화하여 마케팅 분석에 활용하는 경우
사례 2 : 아무런 동의를 받지 않고 웹사이트에서 개인정보를 수집한 후, 익명화하여 마케팅 분석용으로 활용하는 경우

- 현행 개인정보보호법에 의할 경우 개인정보를 수집한 후 익명화하는 것이 허용되는가?
  - 몇 가지 견해가 가능함.
  - 첫째는 익명화는 개인정보의 처리가 아니므로 개인정보보호법의 규율 대상이 아니며, 적법하게 허용된다는 견해.
  - 둘째는 익명화도 허용되지 않는다는 견해.
  - 셋째는 연구나 통계처리 목적의 제공만 허용된다는 견해(개인정보보호법 제18조 제2항 제5호[19]의 반대해석).

[19] 18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.
② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

- 물론, 개인정보주체에게 적법한 동의를 받지 않고 개인정보를 수집했다면 그 수집 자체가 불법이기 때문에 이를 익명화했다고 해서 적법해지는 것으로 볼 수는 없다.

다. 동의를 받고 처리한 개인정보를 익명화하여 제3자에게 제공하는 것은 허용되는가?

(1) 개인정보보호법 제18조 제2항 제5호의 적용

- 예를 들어 통신사에서 개인정보주체에게 동의를 받지 않고 고객들의 개인정보를 익명화하여 영리 목적으로 제3자에게 판매하는 경우, 이는 적법한가?
- 개인정보보호법 제18조 제2항 제5호는 개인정보를 익명처리하는 경우에 제공될 수 있는 경우를 통계작성이나 학술연구 등의 목적에 필요한 경우로 한정하고 있다.
- 이는 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우와 그 외의 목적으로 구분하여 전자는 허용하고, 후자는 금지하는 규정으로 해석해야 한다.

(2) 프라이버시 침해

- 개인을 식별할 수 있는 개인정보가 아니더라도 사생활의 비밀이 침해되는 경우가 있을 수 있음.

> 구체적인 사례
> 건강보험심사평가원의 경우 : 수집된 개인정보를 특정 개인을 알아볼 수 없는 형태로 가공하여 학술연구나 통계작성 목적으로 연구기관에 제공하는 경우는 허용됨.
> 의약품 판매 목적으로 하는 제약회사나, 보험상품 개발을 목적으로 하는 보험회사에 제공하는 경우는 허용되지 않음

(3) 개인정보처리자가 수집한 개인정보를 익명화하여 광고 제공이나, 신상품 개발에 사용할 목적인 제3자에게 제공하려는 것은

- 개인정보보호법은 개인정보 주체의 개인정보자기결정권을 실질적으로 보장하기 위하여 개인정보처리자가 익명화하더라도 해당 개인정보를 통계 목적이나 연구 목적 등으로 제공하는 경우 외에는 제공할 수 없도록 규정함.

7, 빅데이터 가이드라인의 비식별화의 정의는 잘못 되어 있다

가. 가이드라인의 비식별화 정의는 적정하지 못함

---

3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

- 비식별화의 정의
  - “비식별화”란 데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별할 수 없도록 하는 조치를 말한다.
- 비식별화라는 용어의 적정성
  - 비식별화라는 것은 과정에 초점을 맞추는 표현임.
  - 회복 불가능하게 또는 회복하는 것이 심하게 곤란하도록 비식별화되었어야만 한다는 관념이 제대로 전달되지 않음.
- 재식별화의 가능성을 ‘쉽게 결합하는 다른 정보’로 한정하는 것은 부당함
  - 가이드라인은 재식별화의 기준을 ‘쉽게 결합하여 재식별이 되지 않기만 하면 비식별화 된 것’으로 봄.
  - 재식별화의 가능성은 ‘쉽게 결합’하여 재식별화가 되는 경우로만 한정해서는 안됨.
- ‘특정’ 개인의 식별
  - 특정 개인으로 식별이 되는 경우만 문제가 되는가?
- ‘식별할 수 없도록 하는 조치’
  - 재식별 가능성 판단의 시점은 현재가 아닌 미래
- 익명화 기술의 재식별화의 가능성에 대한 고려가 없다.

나. 가이드라인은 비식별화 처리 후 재식별화되더라도 처리중단이 아닌 재비식별화를 하도록 함[20]

- 특히 가이드라인은 “비식별화 조치된 공개된 정보 및 이용내역정보를 조합·분석 등 처리하는 과정에서 개인정보가 생성되지 않도록 하여야 한다. 다만, 개인정보가 생성되는 경우에는 지체없이 파기하거나 비식별화 조치를 취하여야 한다.”고 함. 이와 같은 태도는 사실상 재식별화가 가능한 경우에도 비식별화된 것으로 인정하는 것임.
- 그러나 비식별화를 했으나 재식별화가 된다면 이는 익명처리가 안된 것임.
- 따라서 필요한 동의를 받지 않았다면 해당 정보처리는 위법한 것이 됨.
- 이 경우 정보처리를 중단하고, 해당 개인정보를 회수하거나 폐기해야 함.
- 그러나 가이드라인은 이 경우 다시 비식별화하도록 하고, 정보처리를 하도록 함.
- 재식별화 될 경우 처리 중지가 아닌 다시 비식별화를 하도록 한 것은 재식별화된 것을 익명화 실패가 아니라고 보기 때문임.
- 이는 개인정보보호법의 규정에 위반되는 것임.

---

[20] 심지어는 한국정보화진흥원이 발간한 ‘개인정보 비식별화에 대한 적정성 자율평가 안내서’에서도 재식별화시 대응조치로 데이터 공개 중단 및 회수, 데이터 제공 및 처리 위탁 중단, 데이터 재식별 위험 통지, 개인정보 유출통지 및 유출신고, 추가적 비식별화 조치를 규정하고 있다.

다. 부득이 용어를 사용한다면 '비식별화'가 아니라 '익명화 조치'라고 표현해야 함

- 재식별의 불가능성을 내포하는 개념으로 국민들에게 익숙한 것은 '익명화 조치'임.
- 비식별화는 오해의 가능성이 있으므로 '익명화 조치'라는 표현을 사용해야 함.

라. 유럽연합이나 해외의 사례도 익명화라는 표현을 사용함

- 해외에서도 'de-identification'이라는 용어가 아닌 'anonymisation'라는 용어를 사용함.
- 예를 들어 영국의 ICO(Information Commissioner's Office)가 발행한 것은 'Anonymisation: managing data protection risk code of practice'(익명화 : 데이터 보호 위험의 관리, 시행지침).

7. 가이드라인은 비식별화만 한다면 개인정보주체의 동의를 받지 않고도 개인정보가 포함된 공개된 정보와 이용내역 정보를 수집, 저장, 조합, 분석할 수 있다고 하는 것은 위법하다

가. 가이드라인의 규정

- 가이드라인은 '정보통신서비스 제공자가 정보 처리시스템을 통해 공개된 정보, 이용내역정보를 수집.저장.조합·분석 등 처리하고자 하는 경우, 개인정보의 보호를 위해 다음 각 호의 조치를 취하여야 한다'고 하면서 '개인정보가 포함된 공개된 정보 및 이용내역정보는 비식별화 조치를 취한 후 수집·저장·조합·분석 등 처리하여야 한다'고 규정함.[21]
- 그리고 가이드라인은 '정보통신서비스 제공자는 다음 각 호의 경우를 제외하고는 이용자의 동의를 받거나 비식별화 조치를 취한 후 이용내역정보를 수집.이용할 수 있다.'고 하여, 비식별화 조치만 하면 이용자의 동의를 받지 않아도 이용내역정보를 수집, 이용할 수 있다고 규정함.[22]

---

[21] 제3조(개인정보의 보호) ① 정보통신서비스 제공자가 정보 처리시스템을 통해 공개된 정보, 이용내역정보를 수집.저장.조합·분석 등 처리하고자 하는 경우, 개인정보의 보호를 위해 다음 각 호의 조치를 취하여야 한다.

1. 개인정보가 포함된 공개된 정보 및 이용내역정보는 비식별화 조치를 취한 후 수집·저장·조합·분석 등 처리하여야 한다.
2. 비식별화 조치된 공개된 정보 및 이용내역정보를 조합·분석 등 처리하는 과정에서 개인정보가 생성되지 않도록 하여야 한다. 다만, 개인정보가 생성되는 경우에는 지체없이 파기하거나 비식별화 조치를 취하여야 한다.

[22] 제5조(이용내역정보의 수집·이용) ① 정보통신서비스 제공자는 다음 각 호의 경우를 제외하고는 이용자의 동의를 받거나 비식별화 조치를 취한 후 이용내역정보를 수집.이용할 수 있다.

1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 이용내역정보로서

- 가이드라인은 “정보통신서비스 제공자가 개인정보가 포함된 공개된 정보를 비식별화 조치한 경우에는 이용자의 동의 없이 수집·이용할 수 있다.”고 하여 공개된 개인정보의 경우 이용자 동의 없이 비식별화 조치만으로 수집, 이용할 수 있다고 규정함.[23]
- 가이드라인이 개인정보가 포함된 공개된 정보와 이용내역 정보를 비식별화만 한다면 개인정보주체의 동의를 받지 않고도 수집, 저장, 조합, 분석할 수 있다는 것은 위법하다.

나. 가이드라인의 비식별화 규정은 개인정보보호법이 배제될 수 있는 익명화 조치로 보기 어려움

- 개인정보가 현재 일시적으로 비식별화되었어도 장래의 식별가능성이 있다면 개인정보보호법이 적용되어야 함.
- 그렇다면 개인정보주체의 동의를 받아야 함.

다. 이용내역 정보는 매우 민감한 정보이고, 공개된 정보도 민감한 정보일 수 있음

- 특히 이용내역 정보(“이용내역정보”란 이용자가 정보통신서비스를 이용하는 과정에서 자동으로 발생하는 서비스 이용기록, 인터넷 접속정보, 거래기록 등의 정보를 말한다)는 개인의 매우 민감한 정보에 해당함.
- 쇼핑 내역, 검색 내역, 통신 내역, 의료 등의 이용내역 정보는 개인의 사상, 종교, 성적 취향, 정치적 신조, 노동조합 가입여부, 인종, 건강, 성생활에 대한 정보 등 매우 민감한 정보를 포함함.
- 공개된 정보(“공개된 정보”란 이용자 및 정당한 권한이 있는 자에 의해 공개 대상이나 목적의 제한 없이 합법적으로 일반 공중에게 공개된 부호·문자·음성·음향 및 영상 등의 정보를 말한다.)도 매우 민감한 정보가 될 수 있음.

라. 당사자 동의 없이 비식별화라는 불완전한 조치로 공개된 개인정보와 이용내역정보를 처리하는 것은 매우 위험하다

경제적.기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 다른 법률에 특별한 규정이 있는 경우

[23] 제4조(공개된 정보의 수집.이용) ① 정보통신서비스 제공자가 개인정보가 포함된 공개된 정보를 비식별화 조치한 경우에는 이용자의 동의 없이 수집·이용할 수 있다. 다만, 이용자의 동의를 받거나 법령상 허용하는 경우에는 비식별화 조치를 취하지 아니하고 수집·이용할 수 있다.

- 이용내역정보의 수집 목적을 넘어서는 이용은 비록 비식별화를 했더라도 문제임.
- 비식별화로 특정 개인이 식별되는 것은 아니지만, 잘못된 추론으로 인해 피해를 입게 되는 경우는 개인정보자기결정권 침해는 아니지만 사생활 침해가 될 수도 있음.

마. 재식별화되었어도 다시 비식별화만 하고, 처리 중지나 데이터 회수를 해야 한다고 하지 않는 것은 위법하다

- 가이드라인은 비식별화 조치된 공개된 정보 및 이용내역정보를 조합·분석 등 처리하는 과정에서 개인정보가 생성되지 않도록 하여야 한다. 다만, 개인정보가 생성되는 경우에는 지체없이 파기하거나 비식별화 조치를 취하여야 한다.고 하여 재식별화가 가능한 비식별화 처리도 비식별화로 보고 있음.
- 재식별화가 된 경우도 회수가 아닌 다시 비식별화조치를 취할 수 있다고 규정함
- 이는 개인정보보호법 위반임.

8. 정보주체의 동의 없는 새로운 정보의 생성 규정도 위법한 규정이다

가. 가이드라인의 규정

- 가이드라인은 “정보통신서비스 제공자는 비식별화 조치하여 수집한 공개된 정보 및 이용내역정보를 정보 처리시스템을 통해 조합·분석하여 새로운 정보를 생성할 수 있다. 다만, 새롭게 생성된 정보에 개인정보가 포함되어 있을 경우, 즉시 파기하거나 비식별화 조치를 취하여야 한다.”고 규정하고 있다.

나. 새로운 정보의 생성

- 프로파일링은 정보의 가공이나 분석 등을 통해서 개인정보주체에 대한 새로운 정보를 만들어낼 수 있다. 그런데 이 과정에서 개인정보자기결정권이 침해될 가능성이 매우 높다.
- 그런데 가이드라인은 비식별화조치를 했다면 아무런 동의 없이도 어떤 정보를 새로 생성하더라도 가능하게 하였다.

다. 이는 위법한 규정이다

9. 비식별화 처리된 공개된 정보와 이용내역정보의 내부적 이용도 위법한 규정이다

가. 가이드라인의 규정

- 가이드라인은 ‘정보통신서비스 제공자는 비식별화 처리된 공개된 정보 및 이용내

역정보를 자신의 서비스 제공업무 수행을 위해 내부에서 이용할 수 있다. 다만, 이용자가 거부 의사를 표시한 때에는 그러하지 아니하다.'고 하여, 비식별화 처리만 하면 공개된 정보와 이용내역정보를 서비스 제공업무 수행을 위해 내부적으로 이용할 수 있게 하고 있다.

나. 내부적 이용의 문제점

- 비식별화의 위험성, 비식별화를 했어도 여전히 개인정보인 가능성이 높다는 점을 고려한다면 정보통신서비스제공자가 자신의 서비스 제공업무 수행을 위해 내부적으로 사용할 수 있도록 하는 것은 문제임
- 특히 서비스 제공업무 수행을 위하여 라는 이용목적도 매우 포괄적임.
- 내부적으로 이용한다는 것은 매우 포괄적임.
- 따라서 비식별화한 경우의 동의 없는 내부적 이용은 매우 위험함.

10. 이용자 동의 없는 제3자 제공

가. 가이드라인의 규정

- 가이드라인은 '정보통신서비스 제공자는 개인정보가 포함된 공개된 정보, 이용내역정보, 생성 정보의 경우, 이용자의 동의를 얻어 제3자에게 제공할 수 있다. 다만, 비식별화 처리된 공개된 정보, 이용내역정보, 생성 정보는 이용자 동의 없이 제3자 제공이 가능하다.'고 하여 비식별화를 하면 제3자 제공이 가능하다고 규정하였다.

나. 제3자 제공에 대한 어떤 안전장치도 없음

- 특히 가이드라인은 제3자 제공에 대해서 최소한의 안전장치도 두고 있지 않다. 예를 들어 이용내역정보를 제3자에게 제공하는 경우 해당 정보가 수집·저장·조합·분석 등 처리되는 사실 및 목적을 이용자가 언제든지 쉽게 확인할 수 있도록 개인정보 취급방침을 통해 공개하여야 한다고 하고 있는데 그와 같은 최소한의 장치도 없다.
- 그리고 정보통신서비스 제공자는 이용내역정보의 수집·저장·조합·분석 등 처리를 거부할 수 있는 방법 및 절차를 마련하여야 한다는 거부권에 대한 규정도 없다..