

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『비식별개인정보의 보호 및 활용에 관한 연구』의 연구결과보고서로 제출합니다.

2010. 8.

연구기관 : 서울대학교

총괄책임자 : 정상조 (서울대학교 법학전문대학교)

공동연구원 : 김종보 (서울대학교 법학전문대학교)

송옥렬 (서울대학교 법학전문대학교)

심영택 (서울대학교 법과대학)

허성욱 (서울대학교 법학전문대학교)

연구조원 : 남구현, 노승민, 박성민, 강민수, 나덕중,

박소영, 이강민, 이재성, 이재훈

(이상 서울대 법대 재학생)

요 약 문

1. 제 목

비식별개인정보의 보호 및 활용에 관한 연구.

Legal review on protection and use of the personally non-identifiable information.

2. 연구의 목적 및 필요성

정보통신기술이 발달하고 유비쿼터스 환경이 진전되면서, 개인정보를 수집하고 활용하는 기술이 발전하고 개인정보가 활용되는 맥락이 다양해지고 있다. 개인에 관한 정보를 수집하는 센서들이 많아졌고, 수집된 정보를 가공하는 기술도 다양해졌으며, 개인정보를 이용한 맞춤형 광고나 서비스도 발달하고 있다.

이에 따라 정보의 효율적인 활용이 이루어지고 기업과 소비자의 효용이 증가하는 사회적 편익도 실현되고 있지만, 한편으로는 개인정보의 무분별한 수집과 이용에 따른 정보주체의 기본권 침해가 커다란 문제로 등장하고 있다. 기술과 환경의 급격한 변화에 따라 개인정보를 둘러싼 기본권 침해의 문제는 더욱 다양하고 심각한 양상을 나타내고 있으며, 앞으로도 개인정보의 보호와 활용을 둘러싼 법적, 정치적, 경제적 분쟁사태가 급증할 것으로 예측된다.

이 연구는 고도로 발달된 유비쿼터스 환경에서 개인정보의 보호와 활용을 조화롭게 달성하는 법정정책적 원칙을 검토·분석하는 하는 것을 목적으로 한다. 특히 이 연구는 ‘비식별개인정보(personally non-identifiable information)’의 활용에 관한 법정정책적 원칙을 제시하는데 중점을 두고 있다. 기존의 연구들은 인터넷 환경에서 개인의 성명, 주민등록번호 등 특정 개인을 식별할 수 있는 ‘식별개인정보(personally identifiable information)’에 대한 보호와 활용에 대해 주로 연구하였다. 즉, 전통적으로 개인정보와 관련하여 문제가 되는 것은 ‘식별개인정보’가

일반적이었고, ‘식별개인정보’에 대해서는 이론 탐구 뿐만 아니라 현행법상 법정책의 설계와 집행이 꾸준히 이루어져 왔다.

하지만 유비쿼터스 환경이 발달하면서 이제는 이름, 주민등록번호, 주소 등 특정 개인을 식별할 수 있는 식별개인정보 뿐만 아니라, 사이트 접속기록, 서비스 이용기록, 관심분야, 구매내역, 결제기록, IP정보 등의 비식별개인정보가 수집되고 있고, 이를 이용한 맞춤형 서비스가 제공되고 있다. 이러한 맞춤형 서비스가 전형적으로 실현되고 있는 영역은 온라인 광고시장이다. 전세계적으로 기업들은 마케팅을 오프라인 방식에서 온라인 방식으로 전환하는 추세에 있으며, 효율적인 마케팅을 위한 수단으로 식별개인정보 이외에도 행태정보, 성향정보, 위치정보와 같이 익명으로 처리되어 그 자체로는 특정 개인을 식별할 수 없는 비식별개인정보를 수집·활용하고 있다. 이로써 기업은 효율적인 마케팅을 달성하고 소비자들은 자신에게 필요한 정보만을 제공받을 수 있는 사회적 편익이 달성되고 있으나, 이에 수반하여 비식별개인정보를 무분별하게 수집·이용·제공함으로써 정보주체의 프라이버시가 침해될 가능성이 높아지고 피해의 규모가 커지고 있는 것이 문제로 대두되고 있다.

그런데 이와 같이 맞춤형 온라인 서비스를 위하여 수집되는 비식별개인정보에 대해서는 현행법상 규율이 불분명한 상태이다. 우선, 비식별개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 ‘개인정보’에 포함되는지에 대해 다툼이 있다. 만일 비식별개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정하는 개인정보에 포함되지 않는다면, 현행법상 비식별개인정보를 활용한 광고에 대해서는 규율의 공백이 있는 상황이 된다. 이러한 상황에서 포털, 광고주, 광고회사 등이 규제를 받지 않고 무분별하게 비식별개인정보를 처리한다면 정보주체의 프라이버시가 심각하게 침해되는 문제가 발생하게 된다. 이와 같이, 규제의 지체가 계속된다면 유비쿼터스 환경에서 비식별개인정보의 보호와 활용이 합리적인 균형점을 찾지 못하고 사회적인 비용이 증가하게 될 것이라는 점에서, 비식별개인정보의 보호와 활용에 관한 현행법의 명확한 해석과 법정책의 선제적인 설계는 매우 시급하고 중요한 과제라고 판단된다.

본 연구는 개인의 행태정보, 성향정보, 위치정보 등의 비식별개인정보까지 정보

의 수집과 활용이 확대되는 현실에서, 이러한 정보활용에 대한 현행법의 태도를 면밀히 분석하고, 온라인 맞춤형 광고의 맥락을 중심으로 법정정책 제언을 시도한 연구이다. 이는 향후 온라인 맞춤형 광고시장에서 문제가 될 수 있는 개인정보 보호 원칙에 대한 연구의 기초이자, 법과 정책의 설계의 기초자료가 될 수 있을 것이라고 기대된다.

3. 연구의 범위 및 내용

본 연구의 내용과 범위는 다음과 같다.

첫째, 비식별개인정보의 개념과 유형을 조사한다. 그리고 비식별개인정보의 종류, 정보가 결합되는 정도, 정보가 공유되는 정도, 정보를 처리하는 기술에 따라 비식별개인정보에 대한 적절한 보호수준이 다를 수 있음을 지적한다. 이는 이후의 논의의 전제를 이루는 근본적인 문제이다. 비식별개인정보의 개념과 관련한 국내외의 문헌을 조사·정리하고, 온라인 맞춤형 광고의 맥락에서 정보의 보호수준을 어떻게 설정하는 것이 적절한지 문제를 제기한다.

둘째, 비식별개인정보를 보호하기 위한 우리나라 현행법률을 살펴본다. 현재 우리나라에서 개인정보를 보호하는 법률은 크게 공공영역과 민간영역으로 이원화되어 있고, 민간영역에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 일반법의 역할을 하고 있다. 온라인 맞춤형 광고는 민간영역의 정보통신서비스 제공자가 비식별개인정보를 기초로 수행하는 것이므로, 이와 관련하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 적용되는지 여부가 검토되어야 한다. 특히, 소비자의 행태정보, 성향정보, 위치정보 등의 비식별개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 ‘개인정보’에 포함되는지를 법해석상 명확히 밝히는 것이 문제된다.

셋째, 개인정보자기결정권(비식별개인정보)을 보호하기 위한 외국의 입법례를

비교법적으로 검토한다. 이는 외국의 입법례를 통해 비식별개인정보의 보호 및 활용에 관한 시사점을 도출하는 것을 목적으로 한다. OCED의 개인정보에 관한 가이드라인(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980), 미국의 개인정보보호법제, EU의 개인정보보호법제를 검토하고, 미국과 EU의 입법례에서 대비되는 부분들을 비교, 분석함으로써 그 함의를 파악하고 시사점을 도출하기로 한다.

넷째, 비식별개인정보의 보호와 활용과 관련된 헌법이론을 검토한다. 이는 비식별개인정보를 활용한 온라인 맞춤형 광고에 대해 우리 헌법이 어떠한 입장을 취하고 있는지를 살펴보는 것으로서, 온라인 맞춤형 광고의 규제에 대한 전제적인 논의라고 할 수 있다. 정보주체로서는 자신에 관한 정보에 대해 개인정보자기결정권, 사생활의 비밀과 자유, 일반적 인격권, 재산권, 통신의 비밀, 신체의 자유 등의 헌법상 기본권을 주장할 수 있다. 그러나 이 가운데 비식별개인정보의 수집 및 활용과 가장 밀접한 관련이 있는 기본권은 개인정보자기결정권이라 할 수 있으므로, 개인정보자기결정권의 의의, 근거, 법적 성질, 효력, 내용, 제한 등을 살펴보기로 한다. 한편 광고주체의 입장에서는 비식별개인정보를 활용한 맞춤형 광고에 대해 광고표현의 자유, 영업의 자유, 재산권, 일반적 행동자유권 등을 주장할 수 있다. 그런데 이 가운데 맞춤형 광고와 가장 밀접한 관련이 있고, 광고 규제에 의해 가장 많은 제한을 받는 기본권은 광고표현의 자유라 할 것이므로, 이를 중심으로 헌법이론을 검토하기로 한다. 온라인 맞춤형 광고와 관련하여서는 정보주체의 개인정보자기결정권과 광고주체의 광고표현의 자유가 충돌하는 것으로 볼 수 있고, 양자를 조화롭게 실현할 수 있는 규범조화적 균형점을 찾는 것이 관건이라 할 수 있다.

다섯째, 비식별개인정보의 보호 및 활용을 위한 특별법을 만드는 경우, 개인정보자기결정권과 광고표현의 자유를 합리적으로 조화시킬 수 있는 균형점이 어디인지를 구획하는 것이 중요하다. 이에 대해 규율이 존재하지 않는다면 비식별개인정보를 이용한 맞춤형 서비스에 대해 계속해서 논란과 분쟁이 반복될 수 있다. 본

연구에서는 이와 관련한 법적 기준을 제시하고, 특히 광고거부권(opt-out)을 행사하는 구체적 방안의 예를 제시하기로 한다.

4. 비식별개인정보의 보호 및 활용에 관한 연구결과

첫째, 비식별개인정보는 그 자체로는 특정 개인을 식별할 수 없도록 익명화되어 처리되는 정보이다. 비식별개인정보에는 사이트 접속기록, 서비스 이용기록, 관심분야, 구매내역, 결제기록, 접속시간대 등의 행태정보, 선호하는 방송매체, 신문, 정당, 시민단체, 정치인 등의 성향정보, IP 등의 위치정보 등이 있다. 비식별개인정보는 이름, 주민등록번호, 주소 등의 식별개인정보에 비해서는 개인의 기본권을 침해하는 정도가 작다는 점에서, 일반적으로 보안수준의 정도가 낮다고 할 수 있다. 그러나 비식별개인정보의 종류, 비식별개인정보를 분석하고 종합하는 정도, 비식별개인정보를 제3자에게 제공·공유하는 정도, 비식별개인정보를 처리하는 기술에 따라 정보의 보안수준이 높아질 수 있다. 즉, 비식별개인정보에 의해서 개인의 사생활과 인격권을 침해될 가능성이 높으면, 그에 비례하여 보안수준이 높아진다고 할 수 있다. 따라서 많은 정보가 손쉽게 결합되고 공유되고 저장되는 유비쿼터스 환경에서는 비식별개인정보 역시 식별개인정보에 준하는 높은 보호를 받을 수도 있다.

둘째, 비식별개인정보가 식별개인정보와 결합되지 않고 익명으로 처리되어 특정 개인을 식별할 수 없는 상태에서 수집되고 활용된다면, 이는 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 ‘개인정보’로 볼 수 없다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 문언에 대해 문리해석, 체계해석, 역사적 해석, 목적론적 해석을 수행한 결과, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 비식별개인정보가 식별개인정보와 결합하여 특정 개인을 식별할 수 있게 된 경우에 한하여 비식별개인정보를 ‘개인정보’로 보고 이를 보호하는 것으로 해석된다. 즉, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 특정 개인이 식별되지 않는 상태에서 익명화되어 처리되는 비식별개인정보의 수집과 활용까지 규제하는 법률은 아니라고 봄이 타당하다. 결론적으로, 비

식별개인정보의 보호와 활용에 대해서는 현행법상 입법의 공백이 존재한다고 판단된다.

셋째, 외국의 개인정보보호법제는 OECD의 개인정보에 대한 가이드라인을 중심으로 공공부문, 민간부문이 이원화된 미국법규와 두 부문이 통합되어 하나로 규율되는 EU의 법규로 구별할 수 있다. 미국과 EU 모두 개인정보와 관련된 정의에 있어선 식별가능한 정보에 한정되어있다는 점에서, 우리나라의 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’에서의 개인정보와 크게 다른 바가 없었다. 비식별 개인정보를 이용한 온라인 맞춤형 광고들에 대하여는 미국 FTC와 EU의 가이드라인이 제시되었는데 식별 개인정보의 수집 및 활용에 있어선 확실한 사전적인 동의(Opt-in)를 받을 것을 요구하고 있었고, 비식별 개인정보의 수집 및 활용에 있어선 사후적으로 수령을 거부(Opt-out)할 수 있는 권리가 소비자에게 주어져야 한다고 하는 점을 알아볼 수 있었다.

넷째, 개인정보자기결정권과 광고표현의 자유가 충돌하는 경우에는 양자를 조화롭게 실현할 수 있는 규범조화적 해석을 시도하는 것이 바람직하다. 개인정보자기결정권과 광고표현의 자유 사이에 우열을 가려서 하나의 기본권을 우선시하고 다른 하나를 전적으로 배척하는 것은 가능하지도 않고 바람직하지 않다. 또한 헌법이 규정하고 있는 여러 가지 가치들이 조화를 이루도록 법률을 제정하고 해석하는 것이 헌법의 정신에 부합하는 해석론이라는 점에서 규범조화적 해석을 모색하고자 한다.

다섯째, 비식별개인정보의 보호 및 활용을 위한 특별법을 만드는 경우, 개인정보자기결정권과 광고표현의 자유를 합리적으로 조화시킬 수 있는 균형점을 구획하는 것이 중요하다. 본 연구에서는 비식별개인정보를 활용한 온라인 맞춤형 광고의 맥락에서 1) 당해 광고가 비식별개인정보에 기초한 광고임을 고지(notice)하고, 2) 정보주체에게 광고의 수령을 거부할 수 있는 권리(opt-out)를 부여하며, 3) 광고의 책임자를 명시하여 책임의 소재를 명확히 하고, 4) 온라인 맞춤형 광고를 감독하

는 집행기관을 두는 것이 적절하다고 제안한다. 이 중의 핵심은 정보주체에게 광고거부권(opt-out)을 부여하는 것인데, 권리행사의 상대방이나 시기, 절차 등 구체적인 내용은 앞으로 더욱 깊이 연구할 필요가 있다고 본다. 향후 본 연구결과를 토대로 세미나를 개최함으로써 관련 사업자들과 소비자들의 의견을 수렴해서 방송통신위원회 및 관련 사업자들이 집행할 수 있는 형태의 가이드라인 또는 자율적 규범을 마련하도록 한다.

SUMMARY

1. Title

Legal review on protection and use of personally non-identifiable information

2. Objective and Importance of Research

Nowadays the context of using personal information is getting more various after the development in ubiquitous computing technology which is used for collecting and using the personal information data. There are a lot of sensors around us which are collecting people's personal information; besides, online behavioral advertisement which is targeting individual consumers is booming due to the development in the technology of processing collected data.

Thanks to this situation, we can achieve efficient use of the information and the total amount of social welfare(including consumer surplus and producer surplus) is getting bigger. However, the infringement of information owner's privacy, which is resulting from indiscriminating collection and use of personal information, has become a socially serious problem. The scope of this problem is getting various and serious. Unfortunately we can predict that legal, political and economic conflicts concerning protection and use of personal information will increase more.

This study is done for reviewing and analyzing the legal principle of harmonizing two things which seems quite contradictory: protection and use of personal information in the highly-developed ubiquitous environment. In particular, this study mainly focuses on suggesting the principle of using personally non-identifiable information. Previous studies have focused on 'personally identifiable information' including name, resident registration number, e-mail address, etc, which can identify the specified individuals. That is, the main

concern relating to the infringement of personal information is usually about 'personally identifiable information. Furthermore, currently law and policy have already been made and enforced as well as the theoretical research.

What makes us worried is that personally non-identifiable information such as site-access records, service-use records, interesting fields, purchase and payment records, IP address, is also collected for providing targeting-individual service like personally identifiable information(name, resident registration number, e-mail address). This sort of service is typical in the advertising market. Nowadays firms are converting their off-line marketing strategy into the online one and striving to collect personally non-identifiable information such as people's behavior, propensity to consume and location information, which is treated anonymously and cannot identify the information owner by itself, for its efficient marketing. By using this advertising strategy entire social welfare has become larger, for firms can achieve efficient marketing and consumers can be easily given the important and self-important information. At the same time, the problem of abuse and misuse of private information has become more serious and the degree of the damage seems overwhelming.

Nevertheless, it seems that the current law which regulates the personally non-identifiable information is unclear. Whether personally non-identifiable information is included in the scope of 'personal information' which is defined in 'The law of facilitating and protecting the use of Information Network', Article 2, Number 6, is on debate. Besides, substantive and procedural principle which deals the treatment(collection, use, provision) of personally non-identifiable information has not been legislated yet. If the delay of making new regulation about personally non-identifiable information continues, our attempt to find a rational balance between protection and use of personally non-identifiable information will come to fail and social cost from this will grow bigger. Therefore, designing the newly-made law policy concerning the protection and

use of personally identifiable information is considered very urgent and important.

Under the circumstances in which personally non-identifiable information is widely used in the real advertising market, this research reviews the various context of personally non-identifiable information usage and tries to give the law and policy proposal in the context of online behavioral advertisement. We are expecting that this research will become a foundation in the research about information protection and online targeting advertisement and be a good reference for law and policy designing.

3. Contents and Scope of the Research

The contents and scope of this research are as follows:

- 1) This research investigates the concept and types of personally non-identifiable information and points out that the level of protection of personal information can vary according to the context where the information is used. This is directly related to the interpretation of 'personal information' which is defined in 'The law of facilitating and protecting the use of Information Network', Article 2, Number 6. We will review and check internal and external references about the concept of personal information and raise the problem of which amount of protection is needed in the context of online behavioral advertisement.
- 2) This research will review Korea's law made for protecting the right of self-determination of personal information. Now, Korean information-protection law is divided into two parts: public sector and private sector, and in private sector "The law of facilitating and protecting the use of Information Network" has set a general rule and standard. Whether "The law of facilitating and protecting the use of Information Network" is applicable will be the first step to determine which law can give criteria

for online behavioral advertising. While interpreting laws, it should be considered that personally non-identifiable information can be included in the scope of 'Personal Information' by definition.

- 3) This research will provide a comparative law approach about foreign legislation about personal information and personally non-identifiable information. This is for providing an implication from the principles of protection and use of personally non-identifiable information in foreign countries. After checking the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, personal information protection law in U.S, and personal information protection law in EU, we will find an implication by comparing the legislation of U.S and EU.
- 4) This research will provide an overview of the theory of the Constitution concerning the protection and use of personally non-identifiable information. By doing this, we can check which position our Constitution will take on the issue of online behavioral advertisement. This will be a main focus on the regulation on the online behavioral advertisement. Information owner can insist in the right of self-determination of personal information, the right of privacy, the general personal right, property right, and the personal liberty. Among these, the most closely related human rights, however, is the right of self-determination of personal information; thus, we will examine the significance, legal basis, effectiveness, contents, and limitation about it. On the other hand, advertisers can insist on the freedom of speech, the freedom of expression in advertisement, the freedom of business, property right, and general basic freedom. By the way the freedom of expression in advertisement is the most closely related and highly regulated among these, so we will primarily focus on the constitutional theory about it. As far as online targeting advertisement

concerned, the two rights are conflicting each other: information owners' self-determination of personal information and advertisers' freedom of expression in advertisement. The most important thing is to find a normative balance between the two things.

- 5) This research also mainly focuses on setting the borderline that can balance the right of self-determination of personal information and the freedom of expression in advertisement well. If the situation that no special law is made for personally non-identifiable information continues, legal and political conflicts about this will repeat. In order to solve this problem, this research will suggest a legal standard and detailed measures in enforcement.

4. Research Results

- 1) Personally non-identifiable information is the information that is treated anonymously and cannot identify the specified person by itself. Compared with personally identifiable information such as name, resident registration number, address and sensitive information such as people's thoughts, beliefs, and medical history, personally non-identifiable information gives us less worry about privacy invasion and therefore the level of protection requested by the Constitution is low. However, it is possible that people's privacy will be invaded more easily by using second information derived and synthesized from personally non-identifiable information than by using personally non-identifiable information by itself. Consequently, higher level of protection should be needed for personally non-identifiable information in the ubiquitous environment that a lot of information is easily gathered and processed.
- 2) If personally non-identifiable information is now treated anonymously and collected and used without identifying specified ones, it cannot be said

that personally non-identifiable information is included in the scope of 'personal information' in the law of facilitating and protecting the use of Information Network", Article 2, Number 6. As 'the law of facilitating and protecting the use of Information Network", Article 2, Number 6' is made for protecting the right of self-determination of personal information in the Constitution and it is based on the Article 17(the freedom of privacy) and the Article 10(General Personal Right), it is reasonable that it is existing only to prohibit the invasion of privacy and defamation of characters. Then, it is right to see that this law doesn't regulate the collection and use of personally non-identifiable information which is collected anonymously without identifying a special person. Even though anonymous information were treated, it would be hard to acknowledge that some person's privacy had been violated.

In our research, what is the most important amongst these is that the consumers must have the right to opt out the advertisement. Furthermore, the details about counterpart, timing and procedure of exercising rights will have to be conducted more deeply afterwards.

5. Policy Suggestions for Practical Use

Based on the foregoing, followings are proposed:

- 1) Analysis of comparative law is centered by OECD guideline on the Protection of Privacy and Transborder Flows of Personal Data of 1980. Foreign countries' legislation of protection of private information is mainly divided into two parts: American law which regulates public and private sector differently, and EU law which regulates both parts together. By comparing the two, we can find out that 'personal information' is defined as 'personally identifiable information' like that of Korean law. As far as online targeting advertisement dealing with

personally non-identifiable information concerned, it is important that ad providers should get the explicit consent from consumers to opt in the collection of personally identifiable information, and the right for consumers to opt out afterwards should be guaranteed for personally non-identifiable information. It is found that those things are common in American FTC guidelines and EU's guidelines.

- 2) It is desired to find a good balance between the two in case that the right of self-determination of personal information and the freedom of expression in advertisement contradict each other. It is not appropriate to put a bigger emphasis on one and to firmly exclude the other, so we are trying to find a balancing-standard interpretation of law, considering the principle of proportion in the Constitutions.
- 3) If it is agreed that the special law for regulating personally non-identifiable information should be essential, it is important to find the equilibrium that can balance the right of self-determination of personal information and the freedom of expression in advertisement. In this research in the context of online targeting advertisement by using personally non-identifiable information,
 - ① It should be notified that this advertisement is based on personally non-identifiable information
 - ② the right for consumers to opt out that advertisement should be provided
 - ③ the person who is in charge of online advertising by using personally non-identifiable information should be specified
 - ④ the institution for monitoring online targeting advertisement should be installed

6. Expectations

Under the circumstances in which personally non-identifiable information is

widely used in the real advertising market, this research will provide summary and characteristics of personally non-identifiable information., where such will be used to provide guidance to new regulations and policies.

목 차

제 1 장 서 론	1
제 1 절 연구의 필요성	1
제 2 절 연구의 목적 및 내용	2
제 2 장 비식별개인정보의 개념과 법적 쟁점 고찰	6
제 1 절 서 론	6
제 2 절 비식별개인정보의 개념과 특성	7
1. 개인정보의 개념	7
가. 서 론	7
나. 개인정보 개념에 관한 기존의 논의	8
2. 개인정보의 유형	10
3. 비식별개인정보의 유형과 수집방식	13
가. 이용자의 검색어를 통한 정보수집	13
나. 이용자의 ID를 통한 정보수집	15
다. 이용자의 위치를 통한 정보수집	16
라. 이용자의 RFID를 통한 정보수집	17
마. SNS 이용을 통한 행태정보 수집	18
4. 비식별개인정보의 특성	20
가. 정보의 종류에 따른 보안수준의 차등화	20
나. 정보의 결합 정도에 따른 보안수준의 차등화	20
다. 정보의 공유 정도에 따른 보안수준의 차등화	21
라. 정보의 처리 기술에 따른 보안수준의 차등화	21
마. 보안환경의 변화	22
바. 소 결	22

제 3 절 비식별개인정보의 활용과 그 한계	23
1. 비식별개인정보의 활용례	23
가. 서 론	23
나. 온라인 맞춤형 광고의 사업자 유형	25
다. 맞춤형 광고의 종류와 개인식별력	28
라. 사업자별 광고유형과 개인식별력	29
2. 비식별개인정보의 활용과 개인정보의 침해 문제	30
가. 서 론	30
나. 개인정보 침해의 유형	31
다. 소 결	34
 제 3 장 비식별개인정보를 보호하기 위한 국내 법률 검토	35
제 1 절 서 론	35
제 2 절 개인정보의 개념에 관한 종합적 법해석	38
1. 문리해석	38
2. 체계적 해석	40
3. 역사적 해석	41
4. 목적론적 해석	43
5. 비교법적 검토	45
가. 서 론	45
나. 미국	46
다. 유럽연합	47
라. 영국	47
마. 일본	48
6. 소 결	48
 제 4 장 개인정보자기결정권의 법적 근거	50
제 1 절 서 론	50

제 2 절 개인정보자기결정권의 개관	51
1. 개인정보자기결정권의 의의	51
2. 개인정보자기결정권의 헌법적 근거	51
3. 개인정보자기결정권의 법적 성질	54
4. 개인정보자기결정권의 효력	55
5. 개인정보자기결정권의 내용	55
6. 개인정보자기결정권의 제한	56
7. 개인정보자기결정권의 제한의 한계	56
8. 사권(私權)으로서의 개인정보자기결정권	69
제 3 절 온라인 맞춤형 광고에 따른 기본권의 충돌	70
1. 서 준	70
2. 광고표현의 자유	72
3. 기본권 충돌의 해결방안	73
가. 기본권충돌의 의의	73
나. 기본권충돌의 해결방안	74
4. 소 결	79
 제 5 장 개인정보자기결정권의 보호에 관한 외국입법례	81
제 1 절 OECD	81
제 2 절 미국	85
1. 미국 개인정보보호 관련 법률의 체계	85
2. 개인정보의 침해와 관련 사례들 살펴보기	90
가. Remsburg v. DocuSearch 사건	90
나. Choice Point 사 사건	90
다. 소비자의 행태정보를 광고주에게 판매하는 마켓플레이스	91
라. 더블클릭(DoubleClick) 사건	93
제 3 절 유럽연합	99
1. 유럽연합 개인정보보호 관련 법률의 체계	99

가. 1981년 조약	99
나. Directive 95/46/EC of 24. October. 1995	100
2. 관련 사례들	104
가. 구글의 Street view에 대한 EU의 제재	104
나. 영국 Phorm 사 사건	106
제 4 절 소 결	107
제 6 장 비식별개인정보의 보호와 활용에 관한 법정책	109
제 1 절 서 론	109
1. 가이드라인의 필요성	109
2. 가이드라인의 효력	110
제 2 절 법정책적 제언	110
1. 개인정보의 범위	110
2. 온라인 맞춤형 광고의 표시(notice)	112
3. 광고거부권(opt-out) 행사의 기회 제공	113
4. 광고책임자의 명시	114
5. 온라인 맞춤형 광고의 감독기구	115
제 3 절 광고거부권(opt-out) 행사의 구체적 방안	115
1. 브라우저상의 쿠키 컨트롤	116
2. Windows Live ID 쿠키 셋팅	117
3. NAI의 제3자 쿠키 거절 기능	117
제 4 절 소 결	118
제 7 장 결 론	120
첨부 : 온라인 행태정보의 보호 및 이용에 관한 가이드라인(안)	124
Abstract	132

CONTENTS

Chapter 1 Introduction	1
Section 1 Needs for this Study	1
Section 2 Objective and scope of this Study	2
 Chapter 2 Concept of Personally Non-identifiable Information (PNII) and Legal Issues	 6
Section 1 Introduction	6
Section 2 Concept and characteristics of personally non-identifiable information (PNII)	7
1. Concept of personal information	7
A. Introduction	7
B. Current discussions on the concepts of personal information	8
2. Types of personal information	9
3. Types and methods of collecting NPI	12
A. Collecting PNII through user's search words	13
B. Collecting PNII through user's ID	14
C. Collecting PNII through user's location	15
D. Collecting PNII through user's RFID	16
E. Collecting behavioral information using SNS	17
4. Characteristics of PNII	19
A. Setting different security levels based on types of information	19
B. Setting different security levels based on an extent of integration of information	19

C. Setting different security levels based on an extent of information sharing	20
D. Setting different security levels based on information processing technology	20
E. Changes in security environment	21
F. Conclusion of the Section	21
Section 3 Use of PNII and its limitations	22
1. Examples of PNII uses	22
A. Introduction	22
B. Types of customized online ad service providers	24
C. Types of customized ads and personal identifiability	27
D. Types of ads of each provider and personal identifiability	28
2. Uses of PNII and infringement of personal information	29
A. Introduction	30
B. Types of infringement of personal information	30
C. Conclusion of the Section	32

Chapter 3 Review of Domestic Laws for Protecting PNII ... 34

Section 1 Introduction	34
Section 2 Overall legal interpretation on the concept of personal information	37
1. Literal interpretation	37
2. Systematic interpretation	38
3. Historical interpretation	39
4. Objective-oriented interpretation	41
5. Comparative legal interpretation	44
A. Introduction	44

B. United States	45
C. European Union	45
D. England	46
E. Japan	46
6. Conclusion of the Section	46

Chapter 4 Legal Basis for Rights to Self-Decide Personal Information 49

Section 1 Introduction	49
Section 2 Overview of rights to self-decide personal information ...	49
1. Significance of rights to self-decide personal information	50
2. Constitutional basis for rights to self-decide personal information ...	50
3. Legal characteristics of rights to self-decide personal information ...	53
4. Validity of rights to self-decide personal information	53
5. Contents of rights to self-decide personal information	54
6. Restrictions on rights to self-decide personal information	54
7. Limitations on restrictions on such rights	55
8. Rights to self-decide personal information as privacy rights	68
Section 3 Conflicts of basic rights due to customized on line ads ..	69
1. Introduction	69
2. Freedom of expression in advertisements	71
3. Solutions to conflicts of basic rights	72
A. Significance of conflicts of basic rights	72
B. Solutions to conflicts of basic rights	73
1). Legal theories	73
2). Case laws	74
3). Discussion	77

4. Conclusion of the Section	78
------------------------------------	----

Chapter 5 Foreign Laws on Protection of Rights to Self-Decide Personal Information 80

Section 1 OECD	80
----------------------	----

Section 2 United States	83
-------------------------------	----

A. Legal structure of protection of personal information in the United States	83
---	----

B. Cases involving infringement on personal information	87
---	----

a) Remsburg v. DocuSearch	87
---------------------------------	----

b) Choice Point allegations	88
-----------------------------------	----

c) Marketplace for selling consumers' behavioral information to ad providers	89
--	----

d) DoubleClick allegations	91
----------------------------------	----

A) Introduction	91
-----------------------	----

Section 3 European Union	96
--------------------------------	----

A. Legal structure of protection of personal information in European Union	97
--	----

a) 1981 Treaties	97
------------------------	----

b) Directive 95/46/EC of 24. October. 1995	97
--	----

B. Related cases	101
------------------------	-----

a) EU's sanction on Google's Street view	101
--	-----

b) Allegations on British Phorm	103
---------------------------------------	-----

Section 4 Conclusion of the Section	104
---	-----

Chapter 6 Legal Policy on Protection and Use of PNII 106

Section 1 Introduction	106
Section 2 Legal and Policy Suggestions	106
1. Scope of personal information	107
2. Notice of customized online ads	108
3. Opt-out provision	109
4. Notice of ads providers	110
5. Supervisory entity for customized online ads	111
Section 3 Detailed measures on exercising rights to opt-out	112
1. Control of cookie on browser	112
2. Setting cookie in Windows Live ID	114
3. Option for refusing third party's cookie in NAI	114
Section 4 Conclusion of the Section	115
 Chapter 7 Conclusion	 117
 Appendix: (Proposed) Guidelines on protection and uus of online behavioral information	 120
 Abstract	 129

표 목 차

[표 2-1] 개인정보의 유형과 종류	11
[표 2-2] Corby (2002)의 개인정보 분류	12
[표 2-3] 비식별개인정보의 종류에 따른 보안수준의 차이	20
[표 2-4] 보안환경의 변화	22
[표 2-5] 개인정보침해유형	33
[표 3-1] 개인정보 보호 관련법제 현황	35
[표 3-2] 개별 분야별 개인정보보호입법과 주요 내용	37
[표 5-1]	82
[표 5-2]	84
[표 5-3]	86
[표 5-4]	87
[표 5-5]	103

그 립 목 차

[그림 2-1] 비식별개인정보의 결합 수준에 따른 보안수준의 차이	20
[그림 2-2] 비식별개인정보의 공유 정도에 따른 보안수준의 차이	21
[그림 4-1] 개인정보자기결정권의 내용-자체제작	55
[그림 6-1] 브라우저상의 쿠키 컨트롤	116
[그림 6-2] NAI의 맞춤형 광고 opt-out 기능	118

제1장 서론

제1절 연구의 필요성

정보통신기술이 발달하고 유비쿼터스 환경이 진전되면서, 개인정보를 수집하고 활용하는 기술이 발전하고 개인정보가 활용되는 맥락(context)이 다양해지고 있다. 개인에 관한 정보를 수집하는 센서들이 많아졌고, 수집된 정보를 가공하는 기술도 다양해졌으며, 개인정보를 이용한 맞춤형 광고나 서비스도 발달하고 있다.

이에 따라 정보의 효율적인 활용이 이루어지고 기업과 소비자의 효용이 증가하는 사회적 편익도 실현되고 있지만, 한편으로는 개인정보의 무분별한 수집과 이용에 따른 정보주체의 기본권 침해가 커다란 문제로 등장하고 있다. 기술과 환경의 급격한 변화에 따라 개인정보를 둘러싼 기본권 침해의 문제는 더욱 다양하고 심각한 양상을 나타내고 있으며, 앞으로도 개인정보의 보호와 활용을 둘러싼 법적, 정치적, 경제적 분쟁사례가 급증할 것으로 예측된다.

전통적으로 개인정보 보호와 관련하여 문제되는 것은 성명, 주민등록번호, 주소 등과 같이 특정 개인을 식별할 수 있는 식별개인정보였지만, 고도로 발달된 유비쿼터스 환경에서는 행태정보, 성향정보, 위치정보와 같은 비식별개인정보의 수집과 활용이 새로운 문제로 등장하고 있다. 현행법상 비식별개인정보를 규율하는 특별법은 존재하지 않는 것으로 보이는데, 이러한 상황에서 만일 포털, 광고주, 광고회사 등이 규제를 받지 않고 무분별하게 비식별개인정보를 처리한다면 온라인상에서 정보주체의 프라이버시가 심각하게 침해되는 문제가 발생할 것이다. 개인의 온라인상에서의 행동 양태가 수많은 센서에 의해 수집되고 분석되고 종합되어서 개인에 관한 상세한 프로필이 만들어지고, 이를 이용하여 특정 개인을 지배하고 통제하는 기술남용이 발생할 수 있다. 이와 같이 유비쿼터스 환경에서 비식별개인정보의 보호와 활용이 합리적인 균형점을 찾지 못하고 프라이버시가 침해되는 사회적 문제가 발생하고 있고, 또 발생할 것으로 예상되는 상황에서, 비식별개인정보의 보호와 활용에 관한 현행법의 명확한 해석과 법정책의 선제적인 설계는 매우 시급하고 중요한 과제라고 판단된다.

제2절 연구의 목적 및 내용

이 연구는 고도로 발달된 유비쿼터스 환경에서 비식별개인정보의 보호와 활용을 조화롭게 달성하는 법정정책 원칙을 검토·분석하는 하는 것을 목적으로 한다. 특히 이 연구는 ‘비식별개인정보(personally non-identifiable information)’의 활용에 관한 법정정책 원칙을 제시하는데 중점을 두고 있다. 기존의 연구들은 인터넷 환경에서 개인의 성명, 주민등록번호 등 특정 개인을 식별할 수 있는 ‘식별개인정보(personally identifiable information)’에 대한 보호와 활용에 대해 주로 연구하였다. 즉, 전통적으로 개인정보와 관련하여 문제가 되는 것은 ‘식별개인정보’가 일반적이었고, ‘식별개인정보’에 대해서는 이론 탐구 뿐만 아니라 현행법상 법정정책의 설계와 집행이 꾸준히 이루어져 왔다.

하지만 유비쿼터스 환경이 발달하면서 이제는 이름, 주민등록번호, 주소 등 특정 개인을 식별할 수 있는 식별개인정보 뿐만 아니라, 사이트 접속기록, 서비스 이용기록, 관심분야, 구매내역, 결제기록, IP정보 등의 비식별개인정보가 수집되고 있고, 이를 이용한 맞춤형 서비스가 제공되고 있다. 이러한 맞춤형 서비스가 전형적으로 실현되고 있는 영역은 온라인 광고시장이다. 전세계적으로 기업들은 마케팅을 오프라인 방식에서 온라인 방식으로 전환하는 추세에 있으며, 효율적인 마케팅을 위한 수단으로 식별개인정보 이외에도 행태정보, 성향정보, 위치정보와 같이 익명으로 처리되어 그 자체로는 특정 개인을 식별할 수 없는 비식별개인정보를 수집·활용하고 있다. 이로써 기업은 효율적인 마케팅을 달성하고 소비자들은 자신에게 필요한 정보만을 제공받을 수 있는 사회적 편익이 달성되고 있으나, 이에 수반하여 비식별개인정보를 무분별하게 수집·이용·제공함으로써 정보주체의 프라이버시가 침해될 가능성이 높아지고 피해의 규모가 커지고 있는 것이 문제로 대두되고 있다.

그런데 이와 같이 맞춤형 온라인 서비스를 위하여 수집되는 비식별개인정보에 대해서는 현행법상 규율이 불분명한 상태이다. 우선, 비식별개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 ‘개인정보’에 포함되는지에 대해 다툼이 있다. 만일 비식별개인정보가 「정보통신망 이용촉진 및 정보보

호 등에 관한 법률」에서 정하는 개인정보에 포함되지 않는다면, 현행법상 비식별 개인정보를 활용한 광고에 대해서는 규율의 공백이 있는 상황이 된다. 이러한 상황에서 포털, 광고주, 광고회사 등이 규제를 받지 않고 무분별하게 비식별개인정보를 처리한다면 정보주체의 프라이버시가 심각하게 침해되는 문제가 발생하게 된다. 이와 같이, 규제의 지체가 계속된다면 유비쿼터스 환경에서 비식별개인정보의 보호와 활용이 합리적인 균형점을 찾지 못하고 사회적인 비용이 증가하게 될 것이라는 점에서, 비식별개인정보의 보호와 활용에 관한 현행법의 명확한 해석과 법정책의 선제적인 설계는 매우 시급하고 중요한 과제라고 판단된다.

본 연구는 개인의 행태정보, 성향정보, 위치정보 등의 비식별개인정보까지 정보의 수집과 활용이 확대되는 현실에서, 이러한 정보활용에 대한 현행법의 태도를 면밀히 분석하고, 온라인 맞춤형 광고의 맥락을 중심으로 법정책적 제언을 시도한 연구이다. 이는 향후 온라인 맞춤형 광고시장에서 문제가 될 수 있는 개인정보 보호 원칙에 대한 연구의 기초이자, 법과 정책의 설계의 기초자료가 될 수 있을 것이라고 기대된다.

본 연구의 구체적인 내용은 다음과 같다.

첫째, 비식별개인정보의 개념과 유형을 조사한다. 그리고 비식별개인정보의 종류, 정보가 결합되는 정도, 정보가 공유되는 정도, 정보를 처리하는 기술에 따라 비식별개인정보에 대한 적절한 보호수준이 다를 수 있음을 지적한다. 이는 이후의 논의의 전제를 이루는 근본적인 문제이다. 비식별개인정보의 개념과 관련한 국내외의 문헌을 조사·정리하고, 온라인 맞춤형 광고의 맥락에서 정보의 보호수준을 어떻게 설정하는 것이 적절한지 문제를 제기한다.

둘째, 비식별개인정보를 보호하기 위한 우리나라 현행법률을 살펴본다. 현재 우리나라에서 개인정보를 보호하는 법률은 크게 공공영역과 민간영역으로 이원화되어 있고, 민간영역에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 일반법의 역할을 하고 있다. 온라인 맞춤형 광고는 민간영역의 정보통신서비스 제공자가 비식별개인정보를 기초로 수행하는 것이므로, 이와 관련하여 「정보통신망

이용촉진 및 정보보호 등에 관한 법률」이 적용되는지 여부가 검토되어야 한다. 특히, 소비자의 행태정보, 성향정보, 위치정보 등의 비식별개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 ‘개인정보’에 포함되는지를 법해석상 명확히 밝히는 것이 문제된다.

셋째, 개인정보자기결정권(비식별개인정보)을 보호하기 위한 외국의 입법례를 비교법적으로 검토한다. 이는 외국의 입법례를 통해 비식별개인정보의 보호 및 활용에 관한 시사점을 도출하는 것을 목적으로 한다. OCED의 개인정보에 관한 가이드라인(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980), 미국의 개인정보보호법제, EU의 개인정보보호법제를 검토하고, 미국과 EU의 입법례에서 대비되는 부분들을 비교, 분석함으로써 그 함의를 파악하고 시사점을 도출하기로 한다.

넷째, 비식별개인정보의 보호와 활용과 관련된 헌법이론을 검토한다. 이는 비식별개인정보를 활용한 온라인 맞춤형 광고에 대해 우리 헌법이 어떠한 입장을 취하고 있는지를 살펴보는 것으로서, 온라인 맞춤형 광고의 규제에 대한 전제적인 논의라고 할 수 있다. 정보주체로서는 자신에 관한 정보에 대해 개인정보자기결정권, 사생활의 비밀과 자유, 일반적 인격권, 재산권, 통신의 비밀, 신체의 자유 등의 헌법상 기본권을 주장할 수 있다. 그러나 이 가운데 비식별개인정보의 수집 및 활용과 가장 밀접한 관련이 있는 기본권은 개인정보자기결정권이라 할 수 있으므로, 개인정보자기결정권의 의의, 근거, 법적 성질, 효력, 내용, 제한 등을 살펴보기로 한다. 한편 광고주체의 입장에서는 비식별개인정보를 활용한 맞춤형 광고에 대해 광고표현의 자유, 영업의 자유, 재산권, 일반적 행동자유권 등을 주장할 수 있다. 그런데 이 가운데 맞춤형 광고와 가장 밀접한 관련이 있고, 광고 규제에 의해 가장 많은 제한을 받는 기본권은 광고표현의 자유라 할 것이므로, 이를 중심으로 헌법이론을 검토하기로 한다. 온라인 맞춤형 광고와 관련하여서는 정보주체의 개인정보자기결정권과 광고주체의 광고표현의 자유가 충돌하는 것으로 볼 수 있고, 양자를 조화롭게 실현할 수 있는 규범조화적 균형점을 찾는 것이 관건이라 할 수 있다.

다섯째, 비식별개인정보의 보호 및 활용을 위한 특별법을 만드는 경우, 개인정보

자기결정권과 광고표현의 자유를 합리적으로 조화시킬 수 있는 균형점이 어디인지를 구획하는 것이 중요하다. 이에 대해 규율이 존재하지 않는다면 비식별개인정보를 이용한 맞춤형 서비스에 대해 계속해서 논란과 분쟁이 반복될 수 있다. 본 연구에서는 이와 관련한 법적 기준을 제시하고, 특히 광고거부권(opt-out)을 행사하는 구체적 방안의 예를 제시하기로 한다. 향후 본 연구결과를 토대로 세미나를 개최함으로써 관련 사업자들과 소비자들의 의견을 수렴해서 방송통신위원회 및 관련 사업자들이 집행할 수 있는 형태의 가이드라인 또는 자율적 규범을 마련하도록 한다.

제2장 비식별개인정보의 개념과 법적 쟁점 고찰

제1절 서 론

개인정보의 보호와 관련하여 종래에는 성명, 주민등록번호, 계좌번호, e-mail 주소, ID, 비밀번호 등 개인에 관한 정태적이고 단선적인 정보의 보호가 주로 문제되었다. 이러한 정보는 그 자체로 특정 개인을 식별할 수 있는 식별개인정보(personally identifiable information)라는 점에서, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정하는 개인정보에 해당한다는 점에 별다른 이견이 없었다.

그런데 최근에는 정보통신기술의 발달과 더불어 유비쿼터스 환경이 발전하면서 행태정보, 성향정보, 위치정보와 같은 이른바 비식별개인정보(personally non-identifiable information)의 보호와 활용이 새로운 문제로 등장하고 있다. 이는 근본적으로 유비쿼터스 환경이 개인에 관한 비식별개인정보를 기반으로 한 맞춤형 온라인 서비스를 지향하면서 발생하는 문제로서, 앞으로 유비쿼터스 환경의 발전과 더불어 문제의 양상이 더욱 확대될 것으로 예측된다.

비식별개인정보를 활용한 맞춤형 서비스가 가장 발달한 영역은 온라인 광고시장이다. 광고주와 광고회사, 포털사이트 등은 마케팅의 효율성을 높이기 위해 일률적이고 무차별적인 광고를 지양하고, 이용자의 선호와 관심에 기초한 온라인 맞춤형 광고를 개발하여 전송하고 있다. 이러한 온라인 맞춤형 광고는 본질적으로 이용자의 관심이나 선호와 관련한 행태정보, 성향정보, 위치정보 등의 비식별개인정보의 수집을 전제로 하고 있으며, 실제로 광고주나 광고회사, 포털사이트 등은 온라인 맞춤형 광고를 위해 이용자에 관한 비식별개인정보를 수집하는 기술들을 사용하고 있다.

그런데 이와 같이 마케팅을 위해 이용자의 비식별개인정보를 수집하고 활용하는 것은 이용자의 프라이버시를 침해하는 것이라는 비판이 강력하게 제기되고 있다. 실제로 비식별개인정보를 수집하는 기술을 사용하면, 온라인에서 이용자가 접속한 사이트, 이용한 서비스, 구매한 물건, 읽은 메일, 활동시간대, 이용자의 위치

등을 수집할 수 있는데, 이와 같이 개인의 일거수일투족이 24시간 파악되고 저장되고 분석된다면 이는 개인의 프라이버시에 대한 커다란 침해가 될 수 있다.

이러한 맥락에서, 우선 비식별개인정보의 개념과 특성을 살펴보고, 비식별개인정보의 활용이 정보주체의 기본권(개인정보자기결정권, 사생활의 비밀과 자유, 일반적 인격권, 재산권, 통신의 비밀, 신체의 자유 등)과 충돌하는 양상을 살펴보기로 한다.

제2절 비식별개인정보의 개념과 특성

1. 개인정보의 개념

가. 서 론

2005년에 ‘지문날인사건’에서 개인정보자기결정권을 인정한 헌법재판소 결정에 의하면, 개인정보란 “개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다.”¹⁾

민간영역에서 개인정보자기결정권을 보호하기 위한 법률인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 개인정보의 개념은 다음과 같다.

“개인정보”란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

1) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정.

이상의 법률 규정과 헌법재판소의 결정을 종합하면, 헌법과 법률에 의해 보호되는 개인정보는 1) 생존하는 개인에 관한 정보로서, 2) 당해 정보에 의해 특정 개인을 식별할 수 있거나, 3) 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보를 말한다.

한편, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조 제1항(정보통신서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다.)은 개인의 사상, 신념, 병력(病歷) 등 개인의 사생활과 인격권을 침해할 소지가 높은 정보들은 원칙적으로 수집을 금지하고 있는데, 이러한 민감정보 역시 다른 정보와 결합하여 특정 개인을 식별할 수 있게 하는 정보라는 점에서 개인정보의 일종에 해당한다.

이상 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 규정하고 있는 개인정보의 유형을 분류하면, 1) 식별개인정보(personally identifiable information) : 당해 정보만으로도 특정 개인을 식별할 수 있는 정보, 2) 비식별개인정보(personally non-identifiable information) : 당해 정보만으로는 특정 개인을 직접 식별할 수 없지만, 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있게 하는 정보, 3) 민감정보 : 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보로 분류할 수 있다.

하지만 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 나와 있는 개인정보의 개념은 일반적, 추상적인 언어로 규정되어 있어서, 그 의미를 분명히 파악하기 위해서는 이를 구체화하는 해석작업이 요구된다. 개인정보의 개념에 관한 기존의 해석론을 간략히 살펴보면 다음과 같다.

나. 개인정보 개념에 관한 기존의 논의²⁾

- 1) 생존하는 개인에 관한 정보란, 개인정보의 주체는 생존하는 자연인(自然人)

2) 방송통신위원회, 정보통신서비스 제공자를 위한 개인정보보호 가이드, 2009.12, 8-10면; 나종연 외, 유비쿼터스 환경에서의 개인정보 활용 및 보호방안 연구, 한국인터넷진흥원, 2009, 44-45면

이라는 의미이다. 따라서 사망했거나 실종선고 등 관계법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 개인정보로 볼 수 없다. 또한 법인 또는 단체의 정보도 개인정보에 해당되지 않는다.

2) 개인에 관한 정보란, 당해 개인에 대한 사실·판단·평가 등 개인에 관한 정보를 말한다. 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 개인정보에 대한 구체적이고 세부적인 기준을 정하고 있지 않으므로 특정 개인과 관련된 모든 정보가 개인정보에 해당된다고 볼 수 있다. 따라서, 개인과 관련된 사실적인 정보(예: 이름, 주소, 주민등록번호, 직업)뿐 아니라 해당 개인에 대한 타인의 의견·평가·견해 등과 같은 주관적인 정보(예: 신용평가정보)도 개인정보로 인정될 수 있다.

3) 식별하거나 식별 가능한 정보란, 개인정보로 인정되기 위해서는 당해 정보가 ‘특정 개인을 식별하거나 식별 가능’해야 한다는 의미이다. 따라서 해당 정보가 이미 통계적으로 변환되어 특정 개인이라는 사실을 식별할 수 있는 인자가 제거되었다면 개인정보라고 할 수 없다. 한편, 해당 정보만으로 개인을 식별할 수 있는 정보뿐 아니라 ‘다른 정보와 용이하게 결합’해서 개인 식별이 가능한 경우도 개인정보에 해당한다. 예를 들어, 혈액형과 같은 정보는 개인마다 고유하지 않고 동일한 유형에 속하는 사람이 많기 때문에 개인정보로 보기 어렵다. 그러나 혈액형이 주민등록번호나 주소 등의 정보와 결합하는 경우에는 특정 개인을 식별할 수 있으므로 개인정보로 볼 수 있다. 따라서 개인과 관련된 일반적인 정보들은 대부분 다른 정보와 결합하면 개인 식별이 가능해지므로, 개인에 관한 거의 모든 정보를 개인정보로 간주해야 한다.³⁾

3) 이상에서 인용한 기존의 해석론은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 개인정보의 개념에 관한 단순하고 초보적인 해석으로서, 이에 의해 비식별개인정보에 관한 현행법의 입장을 구체적으로 파악하는 것은 불가능하다. 그러므로 개인정보의 개념에 관한 입체적, 종합적인 해석이 요구되는데, 이에 대해서는 항목을 나누어 제3장에서 서술하기로 한다.

2. 개인정보의 유형

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 개념 정의에 따를 때, 개인정보로 분류될 수 있는 정보로는 다음과 같은 것들을 생각할 수 있다.

구 분	개인정보의 종류
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학적사항, 기술자격증 및 전문면허, 이수한 훈련프로그램, 동아리 활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 상점 및 건물 등
동산정보	보유현금, 저축현황, 현금카드, 주식, 채권 및 기타 유가증권, 수집품, 고가의 예술품, 보석, 자동차, 기타 소유 차량
소득정보	현재 봉급, 봉급경력, 보너스 및 수수료, 기타 소득의 원천, 이자 소득, 사업소득
기타수익정보	보험(건강, 생명 등), 가입현황, 회사의 관공비, 투자 프로그램, 퇴직프로그램
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행 평가기록, 훈련기록, 출석기록, 상벌기록, 성격, 테스트결과, 직무태도, 휴가, 병가
법적 정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트정보
조직정보	노동조합가입, 종교단체가입, 정당가입, 클럽회원

통신정보	전자우편, 전화통화내용, 로그파일, 쿠키
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여 기록, 도박성향 등

[표 2-1] 개인정보의 유형과 종류⁴⁾

이러한 개인정보의 분류는 유비쿼터스 환경이 발달하더라도 근본적으로 변화하지는 않을 것으로 예상된다. 또한 외국의 연구에서도 개인정보의 분류가 거의 유사하게 이루어지고 있는데, 관련 자료를 인용하면 다음과 같다.

데이터 유형			하위 유형과 사례	
정태정보	아이덴티티	오프라인	생체정보	지문, 홍채, 인종, 키 등 신체적 특성 및 DNA
			경제정보	계좌정보, 신용카드 번호 등
			법적 정보	주민등록번호, 여권번호, 운전면허번호 등
			사회적 정보	종교여부, 가입 중인 동호회
			관계적 정보	자녀, 부모, 배우자에 대한 정보 등
			부동산 관련 정보	집, 직장 주소 등
		온라인	디지털 아이덴티티	ID, 이메일주소, 사용자명, IP 주소 등
	자산	유형자산	재산	부동산, 차량, 휴대전화 보유 여부 등, 주식, 계좌 잔액 등
동태정보	통시적 데이터	낮은 수준	거래내역, 여행기록, 통화내역 등	
		높은 수준	유비쿼터스 환경에서 수집된 로그 데이터	
	실시간 데이터	위치정보 등의 유비쿼터스 환경에서 수집된 데이터		
파생정보	분석	시간의 흐름에 따라 수집되고 분석된 데이터		

4) 김범수 외, 『개인정보보호 및 이용의 현황과 사례』, 한국학술정보, 2008, 168-169면

	데이터	○ 경제적 데이터 : 매달 잔고의 흐름, 새로운 제안에 대한 응대 패턴 ○ 사회적 행동 : 약물 사용, 위법 사항, 가족 특성 등 ○ 취향 : 소비패턴, 계층에 따른 아이템으로 분류(구매 설득)
	통합 데이터	다른 데이터와 결합된 개인 정보 ○ DNA 분석 : 정신질환을 포함한 유전질환 발병 가능성 ○ 다자간 연계 데이터 : MAC 어드레스를 제공하는 기기들의 위치로 현재 위치 및 활동 시간을 추정

[표 2-2] Corby (2002)의 개인정보 분류⁵⁾

이와 같은 개인정보에는 성명, 주민등록번호, 주소, 화상(畫像) 등과 같이 특정 개인을 식별할 수 있는 식별개인정보(personally identifiable Information)도 있고, 당해 정보만으로는 특정 개인을 식별할 수 없지만 다른 정보와 결합하여 특정 개인을 식별할 수 있는 비식별개인정보(personally non-identifiable information)도 있다.

여러 차례 언급한 바와 같이, 유비쿼터스 환경에서는 맞춤형 서비스를 제공하기 위해 개인의 관심과 선호에 관한 비식별개인정보를 수집하고 활용하는 것이 불가결하다. 현실에서도 비식별개인정보를 활용하는 기술과 서비스가 개발되어 활용되고 있으며, 기술과 서비스의 수준이 나날이 발전하고 있다. 그러나 이에 따라 정보주체의 개인정보자기결정권과 프라이버시가 침해되는 문제도 발생하고 있다. 이러한 상황에 대한 법적 규율을 설계함에 있어서는 기본적으로 비식별개인정보의 유형이나 특성에 대한 연구가 이루어질 필요가 있다. 이하에서는 유비쿼터스 환경에서 비식별개인정보를 활용한 온라인 맞춤형 광고가 발달하고 있는 현실에 착목하여 비식별개인정보의 개념과 법적 쟁점에 관한 상세한 분석을 수행하기로 한다.

5) Corby, J. M., "The Case for Privacy, Information Systems Security", 11(2), 2002.(나종연 외, 2009, 66면에서 재인용).

3. 비식별개인정보의 유형과 수집방식

비식별개인정보(personally non-identifiable information)는 익명화되어 처리되는 정보로서 당해 정보만으로는 특정 개인을 직접 식별할 수 없지만 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있게 하는 정보이다.

비식별개인정보의 종류는 매우 다양한데, 위의 [표 2-1]에서 일반정보를 제외한 나머지 정보는 대부분 비식별개인정보라고 할 수 있다.

온라인상에서 마케팅을 위해 이용되는 비식별개인정보는 크게 행태정보, 성향정보, 위치정보로 분류할 수 있다. 행태정보는 사이트 접속기록, 서비스 이용기록, 관심분야, 구매내역, 결제기록, 접속시간대 등 온라인상에서 이용자의 행동 양태를 알 수 있게 하는 정보이다. 성향정보는 이용자가 선호하는 방송매체, 신문, 가입한 정당, 시민단체, 노동조합, 지지하는 정치인 등 이용자의 정치적, 철학적인 성향을 파악할 수 있게 하는 정보이다. 위치정보는 IP, 스마트폰 위치 등 이용자의 위치를 추적할 수 있게 하는 정보이다.

광고주, 광고회사, 포털사이트 등의 정보통신망서비스 제공자는 이러한 정보를 통해 이용자의 행태, 성향, 위치 등을 파악하여 맞춤형 서비스를 제공할 수 있다. 이러한 비식별개인정보의 수집 및 활용과 관련해서는 여러 가지 법적 문제점이 있는 것으로 지적되고 있는데, 우선 여기에서는 비식별개인정보의 수집방식에 대해서 몇가지 유형별로 살펴보도록 한다.

가. 이용자의 검색어를 통한 정보수집

1) Yahoo 오버츄어

인터넷 검색사이트에서 특정 키워드를 검색한 사람들을 대상으로 광고주의 사이트가 노출되도록 한다. 따라서 판매자가 불특정 다수에게 광고를 하는 것이 아니라, 특정 키워드를 검색하는 '찾아오는 고객'에게 광고를 하게 된다. 광고비는

클릭당 단가를 산정하는 PPC(Pay per click) 방식으로 이루어져, 이용자가 광고를 클릭해서 광고주의 웹사이트로 이동하였을 경우에만 광고주가 대금을 지불하게 된다.

이러한 광고 서비스를 이용하여 이용자의 검색어 및 광고클릭 등에 관련하여 제한적으로 수집하게 된다. 이용자가 누구인지에 대한 정보는 필요하지 않고, 그 순간 사용된 검색어와 클릭된 해당사이트에 대한 정보만 수집하면 되므로, 공급자의 정보 수집 정도는 낮은 편이다.

2) Twitter 광고 - promoted Tweets

2010년 4월 트위터도 실시간 검색에 검색광고를 붙이는 광고 플랫폼 promoted Tweets를 출시하였다. 이용자가 자신의 트위터에서 특정 검색어를 입력하면 해당 검색어에 대한 광고를 구매한 회사의 트위터 최신 글을 소개해주는 방식이다. 기존에는 관련 사이트 정보나 확인된 광고 문구만을 보여준 것과 달리, promoted Tweets는 이용자에게 광고주의 트위터 최신 글을 소개함으로써 해당 시점에 맞는 동적인 광고가 가능하다.

현재에는 이용자의 검색어와 이용자의 반응을 체크하기 위하여 클릭·해당 트윗에 대한 리플레이 정보 등을 수집하고 있어, yahoo의 오버추어와 비슷한 정도의 정보 수집 정도를 보인다. 하지만 향후에는 해당 이용자가 자주 올리는 주제나 이용자의 위치, 해당 이용자가 following하고 있는 사람들의 관심사 등에 기초하여, 이용자의 트위터 타임라인 중간에 promoted Tweets를 노출하는 광고를 진행할 예정이라고 한다. 이럴 경우 이용자에 대한 행태 분석이 더 세밀하게 이루어지게 된다.

3) Google 애드워즈

Yahoo 오버추어와 유사하게 광고주가 선택한 키워드 중 하나가 검색되면, 해당 검색결과 옆에 광고주가 원하는 광고를 표시하는 서비스이다. Google 애드워즈

는 또한 메일 서비스(gmail)를 통한 광고도 진행한다. 메일의 콘텐츠를 검색하여 메일의 중요 단어를 검색 키워드로 삼아 해당되는 광고를 화면 일부분에 보여준다. 메일에서의 키워드 광고는 이용자의 ID를 통한 행태정보 수집과 결합되어, 한 이용자에게 대한 메일 내용의 수집·분석이 필요하게 된다.

4) Google 애드센스

웹 페이지의 콘텐츠를 자동으로 크롤링하여 사이트의 방문객이나 콘텐츠 내용을 분석하여 그에 맞는 광고를 게재하는 서비스이다. Google Admob, Apple iAd도 비슷한 광고 서비스이다. 이들은 광고를 웹 페이지 또는 애플리케이션에 끼워 넣기 위한 작은 코드조각인 Code Snippet을 통해 콘텐츠 소비 패턴, 사용자 유입 패턴 등을 수집한다.

나. 이용자의 ID를 통한 정보수집

가입 시 입력한 ID를 통해서 이용자를 식별하고, 이용자에게 대한 행태정보를 수집하는 방식이다. 하나의 사이트에서 중복되는 ID가 없어 하나의 ID는 한 이용자를 특정지을 수 있다. 따라서 이용자가 로그인 후 사이트에서 움직이는 행태 정보를 수집하여, 해당 이용자에게 대한 정보를 분석하여 그에 맞는 메일 내용을 통한 맞춤형 광고, 구매 내역을 통한 맞춤형 광고 등을 하는 것이 가능하다. 대표적인 예로는 Amazon이 있다. 또한 IPTV 맞춤형 광고의 경우에도 IPTV 서비스 사업자가 이용자를 식별할 수 있고, 그렇게 식별된 이용자의 시청 경향 등을 통해 광고를 한다는 점에서 ID 기반 맞춤형 광고로 볼 수 있다.

우리나라의 경우, 대부분의 사이트가 가입 시 주민등록번호의 입력을 요하기 때문에 ID라는 비식별 정보가 식별되는 개인정보와 연관될 수 있다. 따라서 우리나라 사이트의 경우 ID 기반 맞춤형 광고에서 사용하는 정보를 식별정보로 보아야 하는지, 비식별정보로 보아야 하는지 경계가 모호하다.

다. 이용자의 위치를 통한 정보수집

1) IP주소

IP 주소 자체에는 위치 정보가 들어가지 않지만, IP prefix(IP주소의 앞부분)의 할당 정보를 결합하여 이용하면 대략적인 위치 정보 검색이 가능하다. 각 통신회사마다 특정 IP prefix를 할당받고, 각 통신회사는 지역별로 IP prefix를 따로 관리하고 있다. 따라서 유동 IP 주소를 사용하더라도, 현재 해당 IP 주소를 사용하는 이용자가 어느 지역에 있는지에 대한 정보를 알 수 있다. 선거 시 포털 사이트에서 해당 지역에 출마한 후보의 배너광고를 띄운 것이 IP 주소를 이용한 서비스가 대표적이다. 하지만 IP 주소를 통한 위치 검색은 그 범위가 넓어 정확도가 떨어지며, 한 이용자를 식별하기에는 부족하다.

2) GPS(Global Positioning System)

GPS는 비행기·선박·자동차뿐만 아니라 세계 어느 곳에서든지 인공위성을 이용하여 자신의 위치를 정확히 알 수 있는 시스템이다. GPS는 현재 단순한 위치정보 제공에서부터 항공기·선박·자동차의 자동항법 및 교통관제, 유조선의 충돌방지, 대형 토목공사의 정밀 측량, 지도제작 등 광범위한 분야에 응용되고 있으며, GPS 수신기는 개인 휴대용에서부터 위성 탑재용까지 다양하게 개발되어 있다. 이렇게 개인 휴대 물품에 탑재되어 있는 GPS를 통하여 개인의 위치 정보를 알아낼 수 있다.

3) WPS(Wi-Fi Positioning Service)

Wi-Fi로 들어오는 무선 AP(Access Point)의 정보를 이용해서 위치값을 얻어내는 서비스로, GPS나 이동통신회사 서비스 이용이 불가능한 단말의 경우도 무선 랜 사용이 가능하면 위치를 얻어낼 수 있다.

WPS는 무선 AP 정보를 얻어내는 기술, 얻어낸 데이터를 최적화하여 데이터베이스를 구축하는 기술, 이용자의 모바일 디바이스에서 필요한 정보를 얻어내는 기술로 구성되어 있다. 우선 스캐닝 차량을 통해서 얻어낸 무선 AP의 MAC (Medium Access Control) 주소 등정보와 GPS를 통해서 얻어낸 무선 AP 위치 정보를 합쳐 무선 AP에 대한 데이터베이스 정보를 구축한다. 그 후 이용자의 모바일 디바이스 근처에 있는 무선 AP들의 정보를 수집하면, 구축된 데이터베이스를 통해 해당되는 무선 AP들의 위치 정보를 결합하여 삼각측량을 통해 해당 모바일 디바이스의 단말기 위치를 측정한다.

4) 기지국

GPS 미장착 핸드폰의 경우, 현재 연결되어 있는 기지국을 이용하여 현재 위치를 파악할 수 있다. 정확한 핸드폰의 위치가 아니라, 연결된 기지국 정보를 통하여 대략적인 위치를 파악하는 것이므로 오차가 있다. 기지국의 통신 영역이 클수록, 핸드폰이 연결된 기지국과 멀리 위치할수록 위치 검색의 오차범위는 커진다. 우리나라 도시의 경우, 고층 건물들이 밀집하여 기지국의 통신 영역이 좁아 오차범위가 적은 편이다. 현재 연결된 기지국에 대한 정보는 통신업체가 관리하고 있다. 통신업체는 해당 핸드폰 단말의 사용자에게 대한 정보를 알고 있으므로, 이러한 정보와 결합되면 식별정보로 볼 수 있다.

라. 이용자의 RFID를 통한 정보수집

RFID(Radio-Frequency IDentification)은 전파를 이용해 먼 거리에서 정보를 인식하는 기술로, RFID 태그와 RFID 판독기가 필요하다. RFID 태그는 고유의 식별번호를 가지고 있으며, 물건에 대한 정보가 들어 있다. 이러한 RFID 태그를 물건에 부착하면, RFID 판독기를 통하여 먼 거리에서도 해당 물건의 정보를 인식할 수 있다.

RFID 판독기가 있으면 먼 거리에서도 한 개인이 가지고 있는 물건들을 알아낼 수 있고, 그러한 정보를 통하여 개인의 성향 등을 파악하여 맞춤형 광고가 가능하

다. 또한 태그는 고유 번호를 가지고 있으므로, 이 고유번호와 한 개인을 연관지면 물건 정보를 통하여 비식별 개인정보로 사용할 수 있다. 이처럼 RFID는 무선 통신의 특성과 RFID 태그의 정보성과 식별성 때문에 개인의 허락 여부와 관계없이 비식별 개인정보가 유출된다는 문제점이 있다.

마. SNS 이용을 통한 행태정보 수집

1) SNS 이용을 통한 행태정보의 종류

Social Network Service (이하 SNS)는 인터넷 서비스 가운데에서도 타인과의 관계 형성을 주목적으로 한다는 특징을 갖는다. 각 사용자는 다른 사용자와 일정한 관계를 맺으며, 다른 사용자의 홈페이지를 방문하여 글을 남기는 등의 방법으로 서로의 관계를 증명한다. SNS를 통해 타인과 관계를 맺는 여러 가지의 행동은 행태정보로써 광고사업자에 의해 활용될 소지가 있다.

SNS에서의 행태정보는 일반적인 인터넷 사용 시에도 나타날 수 있는 사용자 자신에 대한 정보와, SNS에서 독특하게 등장하는 타인과 맺는 관계에 대한 정보로 나눌 수 있다.

가) 사용자 자신에 대한 정보

사용자 자신에 대한 정보는 다시, 가입할 때 입력해야 하는 정보와 가입 후에 작성하는 정보로 나눌 수 있다. 가입할 때 입력해야 하는 정보로는 이메일과 이름, 생년월일, 성별이 있으며, 한국의 경우에는 대개 주민등록번호나 거주지 주소 등의 정보를 추가로 요구하는 경우가 많다. 가입 후에 작성하는 정보로는 남에게 자신을 알리기 위해 작성한 프로필, 본인이 작성한 글 및 사진 등이 있다. 타인이 나를 인식하기 위한 이름이나 성별, 나이, 기본 프로필 정도의 정보는 공개해야 하겠지만, 그 외의 이메일 등의 정보는 굳이 공개할 필요가 없을 것이다. 또 한, 사용자는 자신이 작성한 글이나 사진 등이 익명의 타인에 의해 읽히는 것을 원하지 않

을 수 있고, 자신과 친분이 있는 일부에게만 글의 열람을 허용하고 싶을 수 있다. 그래서 이름과 성별, 본인이 작성한 기본 프로필 등을 제외한 기타 정보에 대해서는 타인에게 공개할지의 여부를 선택할 수 있게 하는 SNS가 대부분이다. 사용자가 일부에게만 열람을 허용한 글은 개인의 사생활을 담고 있을 가능성이 더 크다고 추측할 수 있다. 이런 면에서 SNS에서의 사용자에 대한 정보는 일반적인 인터넷 상의 사용자에 대한 정보에 비해 프라이버시 침해의 위험성이 더 크다.

나) 타인과의 관계에 대한 정보

SNS는 타인과의 소통을 전제로 하기 때문에 SNS의 사용은 필연적으로 타인과의 관계에 대한 정보를 생산하게 된다. 사용자가 가입한 SNS 내의 모임의 종류나, 친구 관계를 맺고 있는 사용자의 목록, 다른 사용자에게 얼마나 많은 글을 남겨주었는지 등이 모두 SNS 내에서 타인과의 관계를 맺음에 따라 생성되는 정보이다. 그런데 SNS측은 이런 정보를 얻음으로써 사용자 및 그 집단에 대한 더 정확한 정보를 얻을 수 있으며, 더욱 정교한 맞춤형 광고를 할 수 있다. 예를 들어, A라는 집단에 가입한 사용자들, 혹은 서로 친한 네트워크를 형성하는 사용자들의 개인정보를 통해 그들의 어느 정도 공통된 취향을 파악할 수 있다고 하자. 그러면 이는 사용자가 속한 집단 전체의 전반적 취향이라고 추측할 수 있으며, 이를 A집단에 속한 사용자들에 대한 맞춤형 광고에 활용할 수도 있다. 이런 정보는 더 효과적인 맞춤형 광고에 도움을 줄 수 있겠으나, 개인이 속한 집단의 실질적인 정보를 제공한다는 점에서, 개인의 소속이나 타인과의 관계에 대한 사생활을 침해할 여지가 있다.

사용자가 어떤 사람과 어떤 관계를 맺고 어떤 모임에 속해있는지의 여부는 개인의 사생활에 해당하는 정보라고 볼 수 있다. 그래서 싸이월드 등 SNS는 사용자는 자신이 어떤 사람과 친구이고 어떤 모임에 속해있는지를 익명의 타인이 알 수 없도록 공개하지 않거나, 일부만 공개할 수 있도록 하고 있다. 한편, Facebook의 경우에는 누가 사용자의 정보에 접근할 수 있는지를 알 수 있도록 해야 한다는 이유에서 사용자와 연결된 네트워크는 모두에게 공개하고 있으며, 그 외의 기

타 정보에 대해서는 사용자의 선택에 따라 공개하지 않을 수도 있다.

4. 비식별개인정보의 특성

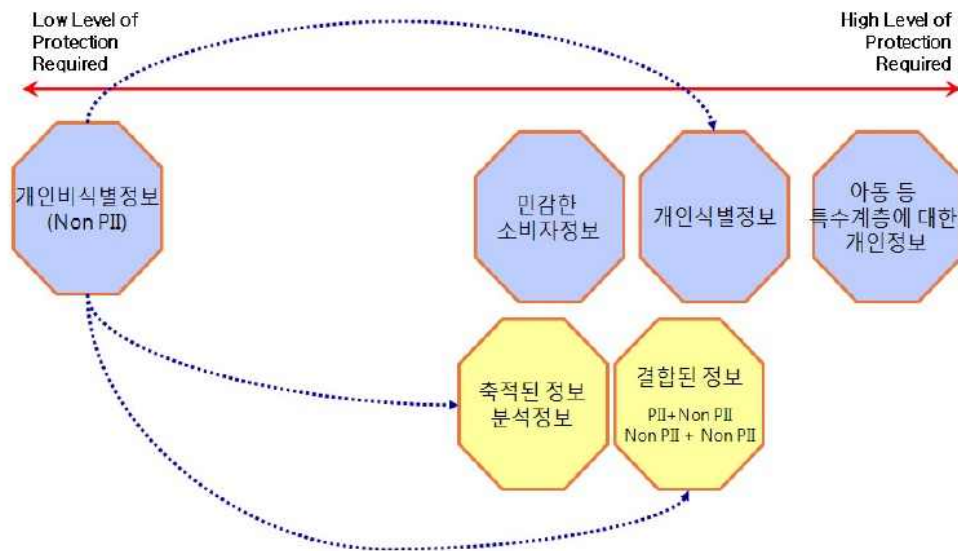
가. 정보의 종류에 따른 보안수준의 차등화

Security Level	General	Surrounding	Vital	Special	서비스 예시
LEVEL 1	나이, 성별, 종교, 기술자격 및 전문면허	주변환경 상황정보 (온도, 습도, 소음)	몸무게, 키, 피부정보, 모발, 가슴둘레	여가활동, 기호식품, 흡연, 관심사, 스포츠 및 오락	맞춤광고 서비스 상품권열안내 서비스
LEVEL 2	이름, 직업, 학력, 학교, 차량정보, 가족구성	공간상황정보 (위치, 속도, 방향)	신체상황정보(채은, 맥박, 혈당), 혈액형, 가족병력	여행정보, 목적지, 클럽 가입정보, 정당가입정보	음성길안내 서비스 생활건강정보 서비스
LEVEL 3	주민등록번호, 봉급액, 사업소득, 단말번호	TBD	장애상황정보(수술, 지병, 장애등급), 개인의료기록	스케줄 정보, 보험가입 정보, 가계지출정보	약자보호 서비스 의료상담 서비스
LEVEL 4	계좌번호, 소유재산 및 부동산정보, 집주소	TBD	지문, 홍채정보, DNA	납세정보, 성생활 정보	홍시큐리티 서비스 납세정보 서비스

TBD : To be determined

[표 2-3] 비식별개인정보의 종류에 따른 보안수준의 차이⁶⁾

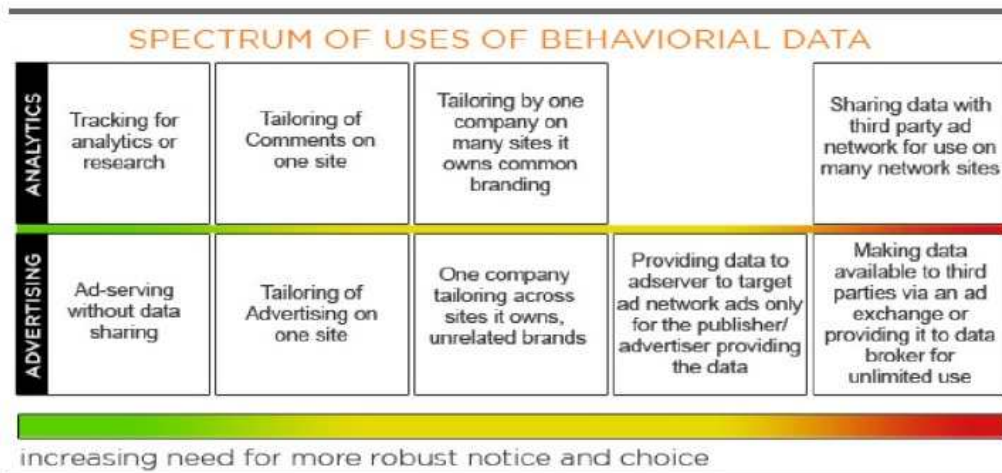
나. 정보의 결합 정도에 따른 보안수준의 차등화



[그림 2-1] 비식별개인정보의 결합 수준에 따른 보안수준의 차이⁷⁾

6) 출처 : 이준규 외, u-city환경에서 맞춤형 서비스 제공을 위한 프로파일기반 개인 정보보호 관리, 정보처리학회논문지 제17-C권 제2호, 2010, 138면.

다. 정보의 공유 정도에 따른 보안수준의 차등화



[그림 2-2] 비식별개인정보의 공유 정도에 따른 보안수준의 차이⁸⁾

라. 정보의 처리 기술에 따른 보안수준의 차등화

정보를 익명화(Anonymization)하는지, 또는 가명화(Pseudonymization)를 하는지에 따라 개인정보보호의 정도가 달라진다. IP 주소나 특정 쿠키 ID(Unique Cookie ID)를 검색정보와 완전히 분리할 것인지, 또는 IP주소나 특정 쿠키 ID의 끝의 몇 자리 수만 삭제하는 부분 삭제를 할 것인지, 또는 역으로 조합이 가능하지 못하도록 기술적 조치를 미리 수집 단계에서부터 취할 것인지, 개인등록정보와 개인행동양태 정보를 함께 보관할 것인지, 또는 수집단계에서부터 따로 보관할 것인지에 따라 개인정보 보호의 정도는 크게 달라진다.⁹⁾

7) 출처 : 나종연 외, 2009, 91면.

8) 출처 : 나종연 외, 2009, 104면.

9) 양지연, 「온라인 맞춤형 광고: 개인정보보호와 정보이용의 균형점을 찾아서, 미국 FTC와 EU의 가이드라인에 비추어」, 『LAW&TECHNOLOGY 제5권 제2호』, 서울대학교 기술과법센터, 2009, 7면.

마. 보안환경의 변화

분 류	내 용
디바이스 측면	개인정보 침해사고의 대상이 PC와 네트워크를 포함한 무선단말, 정보 가전 등 다양한 디바이스로 확대됨
침해 가능성의 증가	개인정보의 범람으로 프라이버시 침해 위험도 커짐
침해 유형의 지능화	비교적 보안등급이 낮은 사용자의 정보(위치, 취미생활)도 유출시 추적을 통해 그 사용자의 신원과 행동 패턴 등을 추론할 수 있음
네트워크 측면	인터넷 침해사고에 취약한 인터넷망에서 발생된 개인정보 침해위협이 BcN을 통해 통신망, 방송망 및 USN까지 확산 가능

[표 2-4] 보안환경의 변화¹⁰⁾

바. 소 결

이상의 이유로, 비식별개인정보에 대해서도 상당한 수준의 보안이 요구된다고 볼 수 있다. 비식별개인정보의 중요성을 과소평가하면 개인정보자기결정권과 프라이버시의 침해가 문제될 수 있다.

이러한 맥락에서 FTC의 가이드라인은 PII와 non-PII의 구분을 상대화하고 있다. 즉, FTC는 전통적인 의미에서의 PII와 non-PII를 구분하는 것은 더 이상 의미가 없으며 PII와 non-PII를 구별하여 사용자 정보의 보호의 기준으로 삼을 수 없다고 하였다. 그 이유로 정보가 수집되고 보관되는 방법에 따라 non-PII와 PII를 조합하거나 연결하는 것이 가능하며, 기술의 발전으로 이전에는 non-PII로 구분되었던 정보로도 지금은 개인을 식별하는 것이 가능해졌기 때문이라고 하였다. 그 예로 IPv6를 들었다. 가까운 미래에 IPv6가 사용되기 시작하면 많은 기기들이 정적인 IP주소(static IP address)를 가지게 될 것이고 이는 곧 IP주소로 특정 기기

10) 출처 : 이준규 외, 2010, 137면.

를 식별하고 나아가 특정 개인을 식별하는 것을 가능하게 하기 때문이다. 또한 정보 그 자체로는 특정 개인을 식별할 수 없지만 온라인상에서의 행동 양태와 검색 정보 등이 축적되면 특정 개인을 식별할 수 있는 정보가 될 수 있다. 또한 한 대의 pc에 여러 사용자가 있을 경우 한 사용자가 방문한 웹사이트나 검색한 정보에 기초해 광고를 전송할 경우 다음 사용자에게 전 사용자에게 대한 민감한 정보가 공유되는 경우가 있을 수 있다. 그러므로 FTC는 온라인 광고를 위해 수집된 정보가 특정 사용자 또는 특정 기기와 “상당히 연결될 수 있는(reasonably could be associated)”되는 경우에는 그러한 모든 정보에 대해서는 FTC 가이드라인의 적용을 받는다는 설명을 통하여 FTC의 가이드라인의 적용을 non-PII까지 확대하였다.¹¹⁾

제3절 비식별개인정보의 활용과 그 한계

1. 비식별개인정보의 활용례

가. 서론

유비쿼터스 환경에서는 비식별개인정보가 다양한 분야에서 활용된다. 예를 들어, 센서를 통해 혈압, 맥박, 체온 등의 건강정보를 병원으로 송신하고 병원에서 이 정보를 분석하여 건강상태를 점검하는 원격진료 서비스(u-Health), 이동단말기를 통해 실시간으로 업계의 동향이나 신제품 소식을 접할 수 있는 맞춤형 뉴스 서비스(u-Business), CCTV로부터 아동이나 노약자, 장애인 등의 위치정보를 확인하여 실시간으로 영상을 확인할 수 있는 약자보호 서비스(u-Home) 등 비식별개인정보의 활용 맥락은 매우 다양하다.

다만 본 연구에서는 온라인 맞춤형 광고의 맥락에서 비식별개인정보의 보호 및 활용에 관한 법정책적 검토를 수행하는 것으로 논의의 범위를 한정하기로 한다. 현재 비식별개인정보를 이용한 맞춤형 서비스가 가장 발달한 분야는 온라인 광고

11) 양지연, 2009, 12-13면.

시장이고, 기본권 침해의 논란이 가장 강력하게 제기되는 맥락도 온라인 맞춤형 광고이며, 본 연구는 이러한 상황에서 온라인 맞춤형 광고를 둘러싼 산업계, 정부, 학계, 시민사회의 이견과 논란을 매듭짓기 위한 연구이기 때문이다.

온라인 맞춤형 광고에서의 개인정보침해 이슈를 이해하기 위해서는 온라인 맞춤형 광고의 구조에 대한 간략한 이해가 필요하다. 맞춤형 광고에 있어 가장 중요한 역할을 하는 사업주체는 바로 웹페이지나 어플리케이션을 통해 직접 이용자에게 해당 서비스를 제공하는 인터넷 기반 맞춤형 어플리케이션 제공 사업자(이하 맞춤형 어플리케이션 사업자)일 것이다. 이들은 자체적으로 이용자들의 행태정보를 일정부분 수집하고, 이를 바탕으로 이용자 별로 맞춤화(customized)된 콘텐츠 및 서비스를 제공한다. 이 때 어플리케이션 사업자가 수집할 수 있는 식별/비식별 개인정보의 종류 및 내용은 다양하며, 회원들의 개인정보와 함께 행태정보를 가공할 수 있는 가능성도 다양하기 때문에, 이들에 대하여 자세히 살펴볼 필요가 존재한다.

한편, 온라인 맞춤형 광고와 관련된 인터넷 산업계에서 광고 플랫폼 사업자를 통한 간접적인 방식의 맞춤형 광고는 점점 더 중요한 비중을 차지하고 있다. 제휴 마케팅(Affiliate Marketing)이라고도 불리는 방식의 이 광고는 온라인 광고 퍼블리셔(이하 퍼블리셔)와 온라인 광고 플랫폼 사업자(이하 광고 플랫폼 사업자)들을 통해 이루어진다. 퍼블리셔는 광고 플랫폼 사업자로부터 맞춤형 광고를 제공받아 자신의 웹페이지 또는 어플리케이션을 통해서 이를 발행(퍼블리싱)하는 사업자를 의미하고, 광고 플랫폼 사업자는 다양한 광고주들로부터 광고들을 수급받아 퍼블리셔들에게 적재적소에 맞춤형 광고들을 제공하는 사업자를 의미한다. 과거 포털이 인터넷 공간상에서 지배적인 영향력을 발휘하였을 때에는 광고의 수급과 발행을 동시에 담당하였으나, 웹2.0 시대의 도래와 함께 블로그를 비롯한 1인 미디어가 대두되고, 아이폰을 필두로 스마트폰의 보급이 가속화되면서 이들을 통한 맞춤형 광고의 시장은 급속하게 팽창하게 하고 있다. 따라서 이들에 대한 적절한 분류와 함께 이들의 비식별개인정보의 수집 및 가공에 관해서 면밀히 분석해 볼 필요가 있다.

나. 온라인 맞춤형 광고의 사업자 유형

1) 맞춤형 어플리케이션 사업자

어플리케이션 사업자는 넓게는 웹이나 스마트폰 어플리케이션(이하 앱)을 통해 이용자들에게 콘텐츠나 서비스를 제공하는 모든 주체를 통칭한다. 그러나 이러한 어플리케이션 사업자들 중에는 자신들이 직접 행태정보를 수집하고, 이를 바탕으로 맞춤형 서비스를 적극적으로 제공하는 사업자들이 있는 반면, 퍼블리셔와 같이 자신의 어플리케이션 내지는 콘텐츠에 관련된 맞춤형 광고만을 소극적으로 제공하는 사업자들도 존재한다. 따라서 이들과 구별하기 위하여 여기서는 전자의 “적극적 사업자”들만을 맞춤형 어플리케이션 사업자로 정의한다. 이들에는 쇼핑몰, 소셜 네트워킹 서비스, 온라인 게임, 포털 등이 포함된다. 통상 이러한 어플리케이션 사업자들은 개인화된 맞춤형 서비스를 제공하기 위하여 계정 등을 만들고 개인정보 및 식별 가능한 행태정보를 수집한다.

2) 퍼블리셔¹²⁾

퍼블리셔(Publisher)란 통상 광고를 발행하는 주체를 의미하는 용어로, 온라인 맞춤형 광고에서는 웹페이지 또는 어플리케이션에 맞춤형 광고를 게시하는 게시자를 의미한다. 과거에는 포털 등 대형 어플리케이션 사업자들만이 주로 이러한 퍼블리싱을 수행하였으나, 최근에는 블로그와 스마트폰 어플리케이션을 중심으로 퍼블리싱이 활발하게 이루어지고 있다. 이들 퍼블리셔들은 자신의 웹페이지 내지는 어플리케이션에 광고 플랫폼 사업장에서 제공한 코드 스니펫(Code Snippet)을 삽입하여 이용자로 하여금 맞춤형 광고에 노출되도록 한다. 코드 스니펫은 접속하는 이용자에게 대한 정보를 수집하여 광고 플랫폼 사업자측 서버로 전달하며, 이를 바탕으로 서버로부터 맞춤형 광고를 가져와 웹페이지 또는 어플리케이션의 화면에 노출시키는 기능을 한다. 이러한 광고는 다음과 같이 퍼블리셔측 웹페이지/어플리케이션에 결합하여 나타난다.

12) 방송통신위원회가 마련한 온라인 행태정보의 보호 및 이용에 관한 가이드라인에서 온라인광고사이트제공자를 의미함.

엔시스의 정보보호 바나나칼라 - 보안전문 블로그

[저녁루크](#) | [태그](#) | [이메일여고](#) | [방명록](#)

인터넷뱅킹, 안전하게 사용할 수 있는 방법은 없을까?

보안기술&트렌드 2009/02/12 11:50

[Google 광고](#)
 [USB보안](#)
 [보안기술](#)
 [CISSP덤프](#)
 [C언어교육](#)
 [보안자격증](#)

최근에 인터넷 뱅킹 해킹으로 인하여 다사한반 사용자들에게 불안한 마음을 던져주고 있습니다. 하지만 늘 보안은 그랑 돌이 게으른 사람, 쉽지않지 않는 사람들이 손해를 보게 되어 있습니다. 따라서 인터넷뱅킹을 안전하게 사용할 수 있는 방법이 없는지 한번 살펴 보도록 하겠습니다.

최근 또 금융기관으로부터 인터넷 뱅킹 해킹으로 인하여 또 한번 언론 기사에 떠돌고 있습니다. 하지만 지금 대부분 인터넷 뱅킹을 하고 있는 사용자입장으로서는 불안 할수 밖에 없습니다. 그리고 보안에 대하여 잘 모르는 사람들은 정말 인터넷 뱅킹을 쳐야 할까. 아니면 다시 일반 창구로 돌아가야 할까 고민 할수도 있겠습니다.

하지만 우리가 편리해진 일상 생활에서 다시 불편한 창구로 돌아가기엔 그리 쉽지 않을것라는 생각이 듭니다. 그러면 정말 인터넷뱅킹을 안전하게 사용할 수 있는 방법이 없을까요? 다 같이 한번 고민해 보아야겠습니다.

▲ 인터넷뱅킹을 안전하게 사용할 수 있는 방법

1. 공인인증서는 PC에 저장하지 말고 반드시 이동저장장치(USB)에 저장을 한다.
2. 보안카드도 소켓하여 PC에 저장하지 말고 따로 휴대하여 사용시마다 눈으로 보고 한다.
3. 자신의 PC에 최신 백신을 설치하여 항상 PC를 모니터링 할수 있도록 백신을 설치한다.
4. 휴대전화 공인인증서 관리 "유니커 서비스" 이용 한다. 또는 OTP 서비스를 받는다.
5. 인터넷뱅킹시에 미체가 되거나 하면 자동으로 SMS 문자가 흡수 있도록 서비스를 신청한다.
6. 신뢰되지 않는 사이트는 합류로 방문하지 않는다.
7. P2P사이트를 통한 신뢰 받지 못한 파일은 절대 다운로드 받지 않는다.

인터넷에 있는 수많은 다양한 보안관련 인터넷뱅킹을 사용 하신수 있겠습니까? 그렇다면 보다 안전하게 편리하게 사용할 수 있는



네이버에서 국가공인정보보호전문가 자격증 발급의 영향이며, 한국CISSP 후보 발표에서 선정되고 있습니다. 본 블로그는 정보보호에 대한 내용을 위주로 구성하고 있습니다. 연락처: sis@sispe.kr HP:010-3000-9300 (오) 엔시스

[Google 광고](#)
 [보안USB](#)
 [보안인증서](#)
 [기밀유출](#)
 [#교육](#)
 [CISSP](#)

공지 [블로그 이동방법](#)

공지 [실시간 전 세계 중지](#)

공지 [미디어\(언론\) 보도자료](#)

공지 [정보보호 관련 사이트](#)

공지 [운영자 소개](#)



4G Internet
by FETOS DESIGN



HonKSS

[Linknow profile](#)

관리자

글쓰기

이러한 퍼블리셔는 통상 블로그나 소규모 웹페이지를 운영하는 사업자 및 단순 어플리케이션 개발자 등 통상 광고 플랫폼 사업자들의 자동화된 서비스에 단순히 가입하여 사용하는 영세 사업자들이다. 이들은 통상 이용자에게 대한 행태정보들을 수집하지 않으며(행태정보는 온라인 광고 플랫폼 사업자 측에서 코드 스크니펫을 통해 바로 수집한다), 통상 식별력이 제거된 통계자료를 광고 플랫폼 사업자로부터 제공받는 것이 보통이다. 때문에 이들은 이용자에게 대한 개인정보를 가지고 있는 경우라 하더라도 이를 제공받은 행태정보와 결합하지 못하는 것이 보통이다. 그러한 의미에서 이들은 앞선 어플리케이션 사업자와 비교하여 ‘소극적’ 맞춤형 마케팅 사업자로 볼 수 있을 것이다.

3) 광고 플랫폼 사업자

광고 플랫폼 사업자는 앞서 언급했듯이 광고주들로부터 온라인 광고들을 제공받아, 퍼블리셔들에게 적재적소에 광고를 배급하는 역할을 하는 주체를 의미한다. 이 과정에서 통상 광고 플랫폼 사업자는 퍼블리셔를 대신해서 직접 행태정보를 수집하고, 이를 바탕으로 맞춤형 광고를 배급하기 때문에, 광고 플랫폼 사업자는 사실상 행태정보 기반의 온라인 광고 제공자의 역할을 하게 된다. (오히려 퍼블리셔는 행태정보를 직접 수집하지 않기 때문에 광고를 낼 공간을 제공하는 소극적인 역할만을 한다.)

우리나라에서는 아직 포털의 영향력이 절대적이기에 이들에 대한 개념이 낯설지만, 블로거 등의 웹페이지 운영자를 퍼블리셔로 삼는 서비스로는 구글의 Adsense, 알라딘의 Thanks to Blogger 등의 맞춤형 광고 서비스가 있으며, 스마트폰 어플리케이션을 퍼블리셔로 삼는 서비스로는 구글의 Admob, 애플의 iAd 등의 맞춤형 광고 서비스가 현재 존재한다. 그리고 포털의 경우에도 검색 키워드를 통한 맞춤형 광고 등은 자신들이 직접 하는 것이 아니라 이들 광고 플랫폼 사업자들을 거쳐서 수행한다(즉, 검색형 광고에 있어서는 네이버 등의 포털도 퍼블리셔의 역할을 수행한다. 이러한 키워드 기반의 맞춤형 광고 서비스에는 구글의 Adwords와 야후의 Overture 등이 있다). 때문에 맞춤형 마케팅에 있어 이들 광고

플랫폼 사업자의 역할은 매우 지대하며, 이들이 수집하는 정보의 범위와 양도 막대하다. 이들은 통상 이용자에게 대한 직접적인 개인정보를 소유하고 있지 않고, 이들이 수집하는 정보는 맞춤형 광고를 제공하는 이상으로 활용되지 않는 것이 보통이나, 이들이 수집하는 정보들은 그 자체만으로도 일정 부분 개인을 식별하는데 사용될 수 있으며, 광고 플랫폼 사업자의 성격상 필연적으로 수집한 정보를 제3자(퍼블리셔와 광고주)들에게 제공·공유하게 된다는 점에서 주의하여 살펴볼 필요가 있다.

다. 맞춤형 광고의 종류와 개인식별력¹³⁾

온라인상에서의 맞춤형 광고는 다음과 같이 크게 세가지로 나뉜다.

첫 번째 유형은 컨텍스트추얼 맞춤형 광고(contextual targeting)라고 불린다. 이 컨텍스트추얼 맞춤형 광고는 사용자가 하나의 웹사이트나 하나의 애플리케이션과의 상호작용을 통해서 얻게 된 정보만을 이용해서 이루어지는 광고를 의미한다. 예를 들면 사용자가 검색창에 검색어를 치면 그 검색어와 관련된 광고를 보여주거나, 사용자가 스포츠 페이지지를 보면 스포츠에 관련된 광고를(배너가 아닌) 텍스트 형태로 보여주는 광고이다. 이 컨텍스트추얼 맞춤형 광고에서는 이전에 수집된 사용자 정보를 사용하지도 않고 사용자에게 대한 정보가 광고분석자료(ad profile)에 수집되지도 않는다.

두 번째 유형은 프로파일 맞춤형 광고(profile targeting)라고 불린다. 이 광고는 일정 기간에 걸쳐 수집되고 광고분석자료에 저장된 사용자 정보를 이용해 광고를 전송한다. 프로파일 맞춤형 광고는 사용자의 온라인 행동양태뿐만 아니라 사용자의 등록정보, 또는 사용자에게 대해 공개된 정보도 이용한다. 개인정보침해의 우려가 가장 많은 광고 형태이다.

세 번째 유형은 행동양태 맞춤형 광고(behavioral targeting)라고 불린다. 이 유형은 프로파일 맞춤형 광고의 한 종류라고 할 수 있는데, 이 광고는 일정 기간 동안 수집되어 광고분석자료에 저장된 사용자의 행동양태에 대한 정보를 사용한다.

13) 온라인 맞춤형 광고의 종류와 구조에 관하여는 양지연, 2009, 4-6면; 나종연 외, 2009, 102-112면 참조.

행동양태 맞춤형 광고에는 사용자의 검색어, 방문한 웹페이지, 클릭한 링크, 그리고 사용자가 본 콘텐츠 등이 모두 포함된다. 행동양태 맞춤형 광고에는 다른 방법을 통해 수집된 사용자 정보는 사용되지 않는다.

이와 같이 광고유형을 분류해보면 비식별개인정보의 가공능력 및 개인 식별력은 유형별로 상당한 차이가 있는데, contextual targeting < behavioral targeting < profile targeting의 순으로 개인식별력이 높다고 보여진다. 따라서 profile targeting의 경우에는 개인정보의 보호필요성이 더 크고 침해위험성도 더 높다고 말할 수 있다.

라. 사업자별 광고유형과 개인식별력

맞춤형 어플리케이션 사업자 및 제휴 마케팅 광고 사업자(퍼블리셔, 광고 플랫폼 사업자)들은 각각 이용자들에게 맞춤형 서비스를 하는 데 있어 하는 역할들이 다르며, 이에 따라 비식별개인정보에 대한 접근 가능성 및 가공능력¹⁴⁾이 달라진다.

개인 블로그나 소규모 게시판, 내지는 단독실행형 스마트폰 어플리케이션 등의 퍼블리셔의 경우에는 ① 콘텐츠 및 서비스의 제공 자체가 행태정보에 기반하여 맞춤형으로 이루어지지 않으며, ② 본래 서비스와는 별도로 수익을 발생시키기 위한 모델로서 맞춤형 광고를 게시하기로 제휴한다. 애초부터 행태정보의 수집을 필요로 하는 서비스 사업자가 아니었기 때문에, 통상적으로 퍼블리셔는 플랫폼 사업자와 제휴를 한 이후에도 직접적으로 행태정보를 수집하거나 수집된 정보를 가공하지 않는다. 보통 퍼블리셔가 얻을 수 있는 따라서 이들의 정보 수집능력 및 가공능력은 매우 제한적이다. 다만, 소규모 게시판의 경우 퍼블리셔가 회원에 대한 개인정보를 가지고 있는 경우가 있는데, 이 경우에도 퍼블리셔가 개인정보와 모든 행태정보를 결합하는 등의 가공능력이 있다고 보기는 어려운 점이 있으며, 따라서 어떤 정보들이 어떻게 결합이 가능한지 살펴보아야 한다. 퍼블리셔들이 광고 플랫폼 사업자로 부터 제공받는 정보들은 가공이 불가능하거나 매우 어려운 경우가 많다. 이는 블로그, 스마트폰 어플리케이션 뿐 아니라 개인정보를 지니고 있는 게시

14) 여기서 “가공”이란, 행태정보를 다른 정보들과 결합시켜 개인에 대한 식별성을 보다 증가시킬 수 있는 모든 종류의 정보처리를 의미한다.

판도 마찬가지이다. 다만, 게시판 사업자 등의 퍼블리셔가 수집한 접속 IP정보와 쿠키를 통한 정보(세션정보, 로그인 정보)들은 회원 가입시 기입한 성명, 주소 등의 개인정보와 결합하여 ‘당해 개인의 신원을 파악할 수 있도록 하는’, 즉 “높은 정도의 식별성”을 가진 정보로 가공할 수 있는 가능성은 남아 있다.

포털과 같은 맞춤형 어플리케이션 사업자는 가장 광범위하게 정보를 수집하고, 이를 가공할 수 있는 능력을 가지고 있다. 예컨대, 맞춤형 어플리케이션 사업자는 이미 이용자들의 개인계정과 관련된 성명, 주소, 주민등록번호, 전화번호, 메일주소 등의 개인정보를 확보하고 있다. 뿐만아니라 맞춤형 어플리케이션 사업자는 어플리케이션 사업자들이 통상 수집하는 행태정보 (IP 주소, 쿠키를 통한 세션정보, 사용자의 웹페이지 이용기록, 컨텐츠 이용 기록, 검색어 기록, 웹브라우저 지문, 휴대기기 위치정보 등)도 수집해서 성명, 주소, 메일주소, 전화번호 등의 개인정보와 결합 또는 가공할 수 있는 최적의 지위에 있다. 따라서, 비식별개인정보의 가공능력 및 개인 식별력은 사업자별로 상당한 차이가 있는데 퍼블리셔 < 광고 플랫폼 사업자 < 맞춤형 어플리케이션 사업자의 순으로 개인식별력이 높고 개인정보의 보호필요성이 더 크다고 말할 수 있다.

2. 비식별개인정보의 활용과 개인정보의 침해 문제

가. 서 론

온라인 맞춤형 광고의 구조를 통해서 살펴보았듯이 소비자들이 인터넷 서버에 접속하여 특정한 사이트에 방문을 하게 되면, 사용자의 컴퓨터는 네트워크 사의 애드서버와 연결이 된다. 애드 서버는 사용자의 컴퓨터에 쿠키를 심어놓게 되고 그것을 통하여 사용자의 정보를 수집하게 된다. 그런데 문제가 되는 것은 이러한 애드 서버들이 수집하는 정보들이 인터넷을 사용하는 사람들의 웹서핑 행동양태에 관한 정보를 무차별적으로 수집하고 있다는 점이다. 대표적으로 소비자 정보를 수집하는 기업인 애드 네트워크(Ad Network)가 수집하는 사용자 정보는 사용자

가 입력한 검색어 뿐만이 아니라 그가 어떤 사이트를 방문했는지 등 웹서핑 행동 양태를 모두 포함하고 있다. 애드 네트워크는 다수의 사이트와 계약을 맺고 있어 각 사이트를 사용하는 사람들의 정보는 누적적으로 애드 네트워크 사의 데이터베이스에 모이게 되고, 정보의 양이 커지는 만큼이나 개인정보침해에 대한 우려는 점점 커지고 있다. 실제로 이러한 광고서버가 사용자의 행동양태에 대한 정보를 축적하는 데 있어 한 기업에 의해 독점이 되지 않는다면 상대적으로 개인정보 침해의 정도가 덜 심각할 수 있겠지만, 정보의 소유가 독점화되어버린다면 엄청난 양의 정보를 소유하는 하나의 기업은 권력집단화 되어버리게 될 뿐만 아니라 소비자의 정보를 남용할 우려도 커지게 되어 개인정보침해와 관련된 문제들이 속출하게 될 가능성이 높아진다.

나. 개인정보 침해의 유형¹⁵⁾

1) 부적절한 접근과 수집

정보주체의 동의가 없는 개인정보수집, 개인정보 수집시 고지 또는 명시적무를 이행하지 않는 행위, 과도한 개인정보 수집 등이 모두 여기에 속한다. 나아가 정보주체의 동의 철회·열람 또는 정정요구에 불응하거나 동의 철회·열람 또는 정정을 수집보다 쉽게 해야 할 조치를 이행하지 않는 행위도 여기에 포함시킬 수 있을 것이다.

2) 부적절한 모니터링

인터넷 마케팅회사들은 쿠키(Cookies)정보를 사용해서 소비자들이 어느 웹사이트를 접속해 얼마나 머무르고 어떤 거래를 하는지를 알아낸다. 정보주체인 개인의 동의 없이 개인의 인터넷 활동을 모니터링하거나, 개인몰래카메라 또는 CCTV를 설치하여 개인의 행동을 감시하는 행위 등도 이에 속한다.

15) 김범수 외, 『개인정보보호 및 이용의 현황과 사례』, 한국학술정보, 2008, 169-171면.

3) 부적절한 분석

소비자나 노동자에게 알려주지 않고 그들의 사적인 정보를 분석하는 행위를 말한다. 부적절하게 수집된 정보와 부적절하게 모니터링된 정보가 분석되면 그것은 당연히 부적절한 분석이 된다. 그러나 정당하게 수집된 정보일지라도 원래 소비자가 동의한 목적 이외의 용도로 부적절하게 분석될 수 있다. 부적절한 분석을 통해 차별적 서비스나, 개인에 대한 통제 강화에 이용할 수 있다.

4) 부적절한 이전

고객에게 알리지 않고 고객의 개인정보를 다른 기업들에게 넘겨주는 행위가 이에 속한다. 제3자 제공, 영업양도 등의 통지의무 불이행도 여기에 포함된다.

5) 원하지 않는 영업행위

주로 인터넷 사용자의 동의나 허가 없이 상품광고메일, 즉 스팸메일을 보내는 행위를 말한다. 이 유형의 프라이버시 침해에는 정크메일(junk mail), 대량 DM 등 영리목적의 광고성 정보 전송이 포함된다.

6) 부적절한 저장

개인정보를 안전하지 못한 방식으로 보관하여 저장된 정보를 외부에 유출하거나, 수집한 개인정보를 목적달성 후 지체없이 파기하지 않는 행위가 이에 해당한다.

개인정보침해유형	관련조문	문제점
부적절한 접근과 수집	정보주체의 동의 없는 개인 정보의 수집	정보주체의 동의가 없을 뿐만 아니라 정보주체가 인식할 수 없는 상황에서 개인

		정보가 수집되어 정보주체가 완전히 자기정보통제권을 상실할 가능성이 큼
부적절한 분석	부적절하게 수집된 정보의 분석, 동의 없는 사적 정보의 분석	부적절하게 수집된 정보의 분석을 통해 개인에 대한 통제와 지배가 심화될 가능성이 큼
부적절한 모니터링	동의 없는 개인의 인터넷 활동 모니터링(쿠키)	부적절한 모니터링을 통해 개인의 프라이버시 등 개인의 생활 전반이 노출될 가능성이 큼
부적절한 이전	개인정보를 제3자에게 양도하는 등 불법적 거래	개인정보를 제3자에게 양도하여 다양한 유형의 개인정보가 불법적으로 거래되거나, 분석된 개인정보가 유통될 가능성이 큼
원하지 않는 영업행위	동의 없는 상품광고, 광고성 정보 전송행위	개인의 특성에 정확하게 조응하는 맞춤형 광고가 동의없이 무차별적으로 유통될 수 있음
부적절한 저장	정보보안의 미흡으로 인한 외부 유출, 정부수집 목적 달성후 개인정보를 파기하지 않는 행위	한 번 수집된 정보가 파기되지 않고 수차의 분석을 통해 다양한 용도로 재활용될 가능성이 큼

[표 2-5] 개인정보침해유형

다. 소 결

기업이 소비자의 개인정보를 수집하고 가공하여 특정한 소비자에게 적합한 맞춤형 광고를 제시하는 것은, 불필요한 광고를 줄이고 기업 내부적으로 보다 저비용으로 효율적인 마케팅을 하는 것이라고 볼 수 있다. 또한, 맞춤형 광고를 통해 절감한 비용을 기업이 R&D와 같은 장기적인 성장의 원동력을 갖추는 데에 사용할 수 있다면 사회 전체적으로 보아도 매우 바람직한 일이 아닐 수 없을 것이다. 다만 소비자에 관한 정보는 개인의 사적인 정보일 뿐만이 아니라, 자기 정보 통제에 관한 권리는 헌법적으로 국민에게 보장된 권리이다. 따라서 기업이 소비자의 정보를 사용하여 맞춤형 광고를 하는 데 있어선 그것이 우리의 헌법과 전체적인 법질서에 위배되는 부분이 없는지 면밀히 검토한 후에야 가능할 일이 될 것이다. 실제로 그러한 검토나 성찰 없이 소비자의 정보가 마음대로 사용되게 된다면, 그로 인한 개인정보의 침해 유형은 더욱 다양해질 것이며 그 피해의 정도도 더욱 심각해질 것이다. 따라서 이제는 개인정보보호와 관련된 우리나라의 법률체계를 살펴보면서, 그것이 현재 문제가 되고 있는 비식별 개인정보에 적용이 되는 것인지, 만약 비식별 개인정보에 적용이 되지 않는다면 우리나라에는 현재 입법의 공백이 있는 것인지 알아보아야 할 것이다.

제3장 비식별개인정보를 보호하기 위한 국내 법률 검토

제1절 서 론

우리나라의 개인정보 보호를 위한 법제는 아래의 표에서 보는 바와 같이 공공 부문과 민간부문으로 구분되어 공·사간에 그 법적 근거 및 집행체계를 달리하고 있다. 먼저, 공공부문에 있어서는 전산처리된 개인정보의 보호에 관한 일반법으로 「공공기관의 개인정보 보호에 관한 법률」이 제정되어 있으며, 그 밖에 전자정부법 및 주민등록법, 국세기본법 등의 개별법에서 개인정보보호에 관한 규정들이 산재하고 있다. 한편, 민간부문에 있어서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정보통신망에서의 개인정보보호에 관한 일반법으로 기능하고 있고, 신용정보에 관해서는 「신용정보의 이용 및 보호에 관한 법률」이, 통신상의 정보 보호에 관해서는 통신비밀보호법이 각기 시행되고 있으며, 그 밖에 정보통신기반 보호법, 금융실명거래 및 비밀보장에 관한 법률 등의 개별법에서도 개인정보에 관한 규정들이 산재하고 있다.

적용분야		법률명	비고
공공부문		「공공기관의 개인정보 보호에 관한 법률」	1994년 제정, 1999년 개정
민간 부문	온라인 사업자	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」	2001년 전문개정, 2002년 개정
기타분야 (개별법)		「신용정보의 이용 및 보호에 관한 법률」, 「위치정보의 보호 및 이용 등에 관한 법률」, 「전자정부법」, 「주민등록법」, 「국세기본법」, 「통신비밀보호법」, 「보건의료기본법」, 「특정범죄신고자 등 보호법」, 「금융실명거래 및 비밀보장에 관한 법률」, 「형법」 등	개별 분야별로 업무상 비밀보호 및 정보보호 규정 산재

[표 3-1] 개인정보 보호 관련법제 현황

개별 분야별로 개인정보보호에 관한 특별규정을 두고 있는 경우로서 대표적인 법률과 관련 규정의 주요 내용을 개략적으로 살펴보면 아래의 표와 같다.

대상 정보	관련 법률	규정 내용
정부 기록 정보	공공기관의 개인정보 보호에 관한 법률	국가, 지방자치단체 등 정부기관 보유의 개인정보 보호
	공공기관의 정보공개에 관한 법률	국민의 알 권리 보장을 위한 공공기록의 공개, 열람
	전자정부법	당사자 의사에 반하는 개인정보사용의 금지 등
	주민등록법	전 국민에 대한 주민등록번호의 부여 등
통신 비밀	통신비밀보호법	우편물의 검열, 전기통신의 감청, 통신사실 확인자료의 제공, 타인 간의 대화를 녹음 또는 청취금지 등 통신관련 사생활의 보호
	통신제한조치의 허가절차 및 비밀유지에 관한 규칙	범죄수사나 개인안보를 위한 통신제한조치의 허가절차
	전기통신사업법	개별이용자에 관한 정보의 공개 및 유용 금지 등
보건 의료 정보	보건의료기본법	보건의료정보의 누출, 변조 금지
	의료법, 전염병예방법 등	업무상 비밀 누설 금지
	생명윤리 및 안전에 관한 법률	유전정보의 보호 등
소 비 자 정 보	정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망사업자의 개인정보보호
	위치정보의 보호 및 이용 등에 관한 법률	위치정보사업자 등의 개인위치정보의 보호
	신용정보의 이용 및 보호에 관한 법률	금융기관, 백화점, 할부회사 등의 고객 신용정보 보호

	금융실명거래 및 비밀보장에 관한 법률	신용정보주체의 열람 및 정정 청구 등
	증권거래법 등	금융실명거래에 따른 금융기관이용자의 개인정보 이용 등
사생활 일반	형법 제316조(비밀침해죄)	봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록 등 특수매체기록에 대한 기술적 침해

[표 3-2] 개별 분야별 개인정보보호입법과 주요 내용

이 중에서 온라인 맞춤형 광고를 규율하는 현행 법률로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 생각할 수 있다. 온라인 맞춤형 광고는 민간영역에서 정보통신서비스 제공자가 비식별개인정보를 활용하여 제공하는 서비스이다. 민간영역에서 개인정보를 보호하기 위한 여러 가지 개별법률들이 있기는 하지만, 현재 문제되고 있는 비식별개인정보(사이트 접속기록, 서비스 이용기록, 관심분야, 구매내역, 결제기록, 접속시간대 등의 행태정보, 선호하는 방송매체, 신문, 정당, 시민단체, 정치인 등의 성향정보, IP 등의 위치정보 등)를 특별히 규율하는 법률은 존재하지 않는다.¹⁶⁾ 따라서 일반법으로서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 적용 여부가 검토되어야 한다. 특히 동법 제2조 제6호의 ‘개인정보’의 개념을 명확히 분석하고 정의하는 작업이 이루어져야 한다.

비식별개인정보가 헌법 및 법률에 의해 보호되는 ‘개인정보’의 범주 안에 포함되는지에 대해서는 개인정보를 보는 관점에 따라 견해가 엇갈리고 있다. 산업계는

16) 위치정보와 관련하여 「위치정보의 보호 및 이용 등에 관한 법률」이 제정되어 있으나, 동법에서 규율하고 있는 위치정보는 그로 인해 특정 개인의 위치를 알 수 있는 정보, 즉 특정 개인인 ‘개인 위치정보주체’를 식별할 수 있는 위치정보를 의미한다(동법 제2조 제2호 및 제3조 제3호 참조). 이와 같은 위치정보는 특정 개인을 식별해낼 수 있다는 점에서 식별개인정보이며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 개인정보에도 해당한다. 다만 「위치정보의 보호 및 이용 등에 관한 법률」은 개인정보의 일종인 위치정보에 대해 특별한 내용을 규정한 특별법인 것이다(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제5조 참조). 현재 문제되고 있는 비식별개인정보 중 하나인 위치정보는 특정 개인을 식별하지 않는 상태에서 익명으로 처리되는 위치정보(가령 인터넷 접속자 1, 스마트폰 이용자 1의 위치)라는 점에서 맥락을 달리 한다.

비식별개인정보를 활용한 맞춤형 서비스는 마케팅 비용을 낮추고 정보 유통의 효율성을 증진시키며 소비자에게도 필요한 정보만을 제공하는 편익이 있으므로 이에 대한 규제나 금지는 바람직하지 않다고 본다. 기업이 시장에서 효율적으로 기능하기 위해서는 비식별개인정보를 자유롭게 활용할 수 있어야 한다고 보며, 이러한 전제에서 비식별개인정보는 현행법상 ‘개인정보’에 포함되지 않는다고 본다. 반면 소비자들은 비식별개인정보의 수집 및 활용은 인터넷 상에서 소비자들의 일거수일투족을 감시하는 것으로서 마케팅을 위해 소비자들의 사생활을 침해하는 것은 정당화될 수 없다고 한다. 비식별개인정보를 분석하고 종합하면, 개인에 대한 거의 완전한 프로필을 만들 수 있고 이는 개인의 사생활에 대한 중대한 침해에 해당하므로, 비식별개인정보 역시 현행법상 ‘개인정보’에 포함된다고 보아 엄격한 규제를 해야 한다고 본다.

이와 같은 상황에서, 현행법의 해석을 둘러싼 논란과 분쟁을 매듭짓고 명확한 행위규범 및 재판규범을 확립하기 위해서는 비식별개인정보가 헌법과 법률에 의해 보호되는 ‘개인정보’의 범위에 포함되는지를 분명히 규명할 필요가 있다. 통상의 규범론적 해석론만으로는 비식별개인정보와 관련하여 현재 문제되고 있는 상황을 해결하는 것이 불가능하다.¹⁷⁾ 이를 위해서 개인정보와 관련된 현행 법률과 법원의 판례를 면밀히 해석해보는 법해석 작업을 수행하기로 한다.

제2절 개인정보의 개념에 관한 종합적 법해석

1. 문리해석

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호에 따르면, “개인정보”란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경

17) 기존의 해석론의 인용과 정리는 제2장 제2절 1.(2) 개인정보 개념에 관한 기존의 논의 참조.

우에는 그 정보를 포함한다)를 말한다.

위 규정 중 비식별개인정보의 개념정의라 할 수 있는 부분은 “해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다”는 부분이다.

위 문언에 대해 언어적, 논리적으로 해석할 수 있는 가능성은 크게 다음의 두 가지로 보인다.

가. 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보라면, 실제로 다른 정보와 결합하여 특정 개인을 식별한 바 없더라도, 특정 개인을 식별할 수 있는 잠재적 가능성이 있는 이상 그 정보를 개인정보로 보아야 한다.

나. 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보가, 실제로 다른 정보와 결합하여 특정 개인을 식별할 수 있게 된 경우에 한하여, 그 정보를 개인정보로 보아야 한다. 이와 달리, 다른 정보와 결합함이 없이 익명으로 처리되어 특정 개인을 식별할 수 없는 상태에서 이용된 비식별개인정보는 동법상의 개인정보로 볼 수 없다.

만일 (1)의 해석을 채택한다면, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정하는 개인정보란 개인에 관한 일체의 정보로서 그 외연이 무한정 넓어질 것이다. 반면 (2)의 해석을 채택한다면 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정하는 개인정보는 그에 의해 특정 개인을 식별할 수 있는 정보로 국한될 것이다.

문리적으로 볼 때, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 문언은 (2)에 따라 해석하는 것이 타당한 것으로 보인다. 문언상 다른 정보와 쉽게 ‘결합하여’ 특정한 개인을 ‘알아볼 수 있는 경우’라는 표현은, 비식별개인정보가 실제로 다른 정보와 결합해서 특정 개인에 대한 식별성을 획득한 경우를 의미한다고 보아야 한다.

이와 달리 비식별개인정보가 다른 정보와 결합할 가능성이 있다는 이유만으로

일체의 비식별개인정보를 개인정보에 포함된다고 해석하는 것은, 법문언의 의미를 가능한 범위를 넘어 지나치게 넓히는 것으로서 타당하지 않은 해석이라 할 것이다.

2. 체계적 해석

체계적 해석의 방법은, 법체계의 일관성을 전제로 관련 법률들을 일관성 있게 해석하는 것을 의미한다. 공공영역에서 개인정보를 보호하기 위한 일반법으로는 「공공기관의 개인정보보호에 관한 법률」이 있다. 체계적 해석에 따르면 「공공기관의 개인정보보호에 관한 법률」이 정하는 ‘개인정보’의 개념과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정하는 ‘개인정보’의 개념은, 양자를 달리 해석해야 할 특별한 이유가 없는 이상 동일하게 해석하는 것이 일관된 태도일 것이다.

「공공기관의 개인정보보호에 관한 법률」 제2조(정의) 제2호는 “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.”라고 규정하고 있다. 이를 분석하면 개인기록(personal record)이나 고유식별자(particular identifying)의 개념을 상정하고 있는 것으로 보인다. 즉 “당해 정보에 포함되어 있는”이라는 문언에 비추어 볼 때 정보의 묶음인 개인기록의 개념을 상정하고 있는 것이고, 또 그 기록 안에 특정 개인을 식별할 수 있는 고유식별자(성명, 주민등록번호, 화상 등)가 포함되어야 한다고 규정한 것이다.

이는 비식별개인정보가 식별개인정보(고유식별자)와 결합하여, 특정 개인에 대한 식별성을 획득한 경우에 한하여, 이를 개인정보의 하나로 본다는 의미로 해석된다. 그리고 이와 같은 해석을 일관되게 관철한다면, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 대해서도, 비식별개인정보가 다른 정보와 결합하여 특정 개인에 대한 식별성을 획득한 경우에 한하여 이를 개인정보에 포함되는 것으로 해석하는 것이 타당할 것이다.

3. 역사적 해석

역사적 해석은 법률을 제정한 입법자의 의사를 추단하여 그에 부합하도록 법률의 문언을 해석하는 방법이다. 입법자의 의사를 추단할 수 있는 자료로는 입법자료, 국회속기록 등이 있다.

그런데 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 관련하여서는 입법자의 의사를 구체적으로 추단할 만한 자료를 발견하기 어렵다. 본법은 “정보통신서비스이용자의 개인정보를 보호하기 위하여 정보통신서비스제공자에 대한 규제를 강화할 목적”으로 제정된 법률이라고 설명되어 있을 뿐,¹⁸⁾ 개인정보의 개념에 비식별개인정보까지 포함되는지, 입법자가 그러한 해석을 의도하였는지에 대해서는 구체적으로 확인할 방법이 없다.

다만, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 관한 기존의 연구를 보면, 입법자의 의사를 추단하는 역사적 해석으로 크게 두 가지 해석이 존재하는 것으로 보인다.

첫째는, 입법자가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 제정할 당시 비식별개인정보에 대해서는 의식을 하지 못했다는 해석이다.¹⁹⁾ 즉, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 동의 요건을 온라인상에서의 모든 개인정보처리(=수집·이용·제공)가 합법적이기 위한 절대적인 기준으로 설정하고 그 위반에 대해 5년 이하의 징역에 처하고 있는데, 이와 같이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 동의 요건을 절대적인 합법성 기준으로 설정한 것은 회원가입시 이용자가 직접 제공하는 정보(이름, 주민등록번호, 전화번호, 이메일주소, 우편주소, 직업, 직장명, 학력, 결혼여부 등)를 수집하는 경우만을 상정한 때문인 것으로 보인다는 것이다. 즉, 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 회원가입시 이용자가 제공하는 개인정보의 수집만을 상정해 놓고 그러한 수집에 대해서 이용자의 사전 동의를 받도록 규정해 놓은 것이고, 회원가입 이후에 수집되는 비식별개인정보, 즉 이용자가 구매한 물건, 결제내역, 접속시간, 이를 분석하여 생성된 소비성향과 구매패턴, 채팅의 내용 등

18) 국회 의안정보시스템, 정보통신망이용촉진등에관한법률개정법률안(대안), 2면 참조

19) 성낙인 외, 2008, 739-745면.

은 고려하지 않은 입법이라는 것이다.

둘째는, 입법자가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 제정할 당시 비식별개인정보에 대해서도 규율을 의도했다는 해석이다.²⁰⁾ 즉, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조 제2항 제1호는

“정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우”에 정보통신서비스 제공자가 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다고 규정하고 있는데, 이것이 비식별개인정보를 염두에 둔 규정이라는 것이다. 즉, 위 사항은 이용자가 요구하는 정보통신서비스를 제공하는 과정에서 서비스 이용기록, 접속 로그(log), 쿠키(cookie), 결제 기록, 이용정지기록, 페이지뷰 내역, 이용 시간대, 검색 사항, 사이트 방문 내역 등의 정보와 같이 불가피하게 생성되어 저장되는 정보에 관한 사항이다. 이러한 정보들은 계약 이행 과정에서 실시간으로 생성되어 수집되지만, 이용자에게 매번 고지하고 동의를 얻는 것에 경제적으로 큰 비용이 들거나 기술적으로 어려운 경우가 많아 그 예외를 인정한 것이다. 다만 위와 같은 정보라 하더라도 이러한 정보들이 수집된다는 사실은 개인정보를 수집할 때 충분히 예측할 수 있으므로, 개인정보를 최초로 수집하는 시점에 ‘수집하는 개인정보 항목’을 통해 명시하고 이용자의 동의(opt-in)를 얻어야 한다. 동의에서 예외가 된다는 사항은, 단순히 생성 시점마다 건별로 동의를 받는 것을 예외로 하는 것이지, 이와 같은 종류의 개인정보를 모두 동의 없이 수집하여 이용할 수 있다는 의미가 아니다.

생각건대, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조 제2항 제1호의 규정을 감안하면, 입법자는 비식별개인정보에 대해서도 부분적으로 규제를 의도한 것으로 봄이 타당할 것이다. 즉, 회원가입시 정보통신서비스 이용자가 제공한 개인정보(식별개인정보 또는 비식별개인정보)에, 이후 정보통신서비스를 이용하는 과정에서 생성되는 비식별개인정보가 결합될 것(Prospective merge)을 예정하고, 이 비식별개인정보에 대해서는 정보통신서비스 제공자가 동의를 받지 않아도 되는 것으로 규정한 것으로 보인다. 방송통신위원회의 가이드라인은 이를

20) 방송통신위원회, 정보통신서비스 제공자를 위한 개인정보보호 가이드, 2009.12, 35-36면

opt-in으로 해석하고 있으나, 명시적으로 “동의 없이 이용자의 개인정보를 수집·이용할 수 있다”고 규정한 조항을 opt-in으로 해석하는 것은 문언에 정면으로 반하는 해석이라는 점에서 의문시된다. 정보통신서비스 제공자가 동의를 받지 않고도 이용자에 관한 비식별개인정보를 수집하여 결합할 수 있지만, 이용자가 이에 대해 거부권(opt-out)을 행사할 수 있는 것으로 해석함이 타당하다고 보인다.

4. 목적론적 해석

목적론적 해석은 법의 목적이거나 법에 내재하는 가치가 무엇인가를 찾아내어 개개의 법률조문을 이에 합치하도록 해석하는 방법을 말한다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정하는 ‘개인정보’의 개념의 외연이 어디까지인지, 비식별개인정보도 모두 ‘개인정보’에 포함되는지에 대해서 목적론적 해석을 수행하면 다음과 같다.

우선, 개인정보는 기본적으로 ‘특정한 개인’, 즉 ‘신원을 확인할 수 있는(identifiable) 개인’에 관한 것이어야 한다고 보는 것이 타당하다. 신원확인이 불가능하게 익명으로 처리되는 정보는 개인정보보호법의 보호대상에서 제외된다. 왜냐하면 개인정보보호법이 종국적으로 보호하고자 하는 것은 정보의 오·남용으로 인해 침해될 특정 개인(정보주체)의 권리나 이익이기 때문이다. 신원확인이 ‘불가능’한 개인정보는 오·남용되더라도 그로 인해 누구의 권리나 이익도 침해되는 바가 없기 때문이다.²¹⁾

한편, 일체의 비식별개인정보를 개인정보로 보아 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해 이를 보호하는 것은 지나치게 엄격한 태도이며, 기존의 인격권 법리를 오해한 것이라 할 수 있다. 그동안 개인의 인격적 이익을 보호하기 위한 민사법제와 형사법제로서 명예훼손법과 사생활보호법이 존재하여 왔다. 또 최근에는 개인의 성명과 초상을 보호하는 법원의 판례가 나오기도 하였다. 그러나 이들 법제와 판례법은 부분적이고 제한적으로만 개인의 인격적 이익을 보호한다.

21) 성낙인 외, 2008, 700면 참조.

명예훼손법은 민사법제와 형사법제 모두 개인에 관한 정보 중 그 개인의 사회적 평가를 저하시키는 사실적 정보를 공개적으로 공표하여 그 개인의 명예를 훼손하는 경우에 적용되는 법제이다. 명예훼손법은 개인에 관한 사실적 정보 그 자체를 보호하고자 하는 것이 아니라 그러한 정보의 공표로 인해 훼손되는 인격적 이익인 명예를 보호하고자 하는 법이다. 그리고 이때의 명예도 개인의 명예감이 아니라 사회적 평가로서의 외부적 명예를 의미한다.

한편 민사법제로서의 사생활보호법은 민사상의 불법행위법으로서 존재하는데, 개인이 숨기고자 하는 은밀한 사생활정보를 공표하거나 또는 개인의 사생활 영역에 무단히 침입하여 평온을 해치는 경우에 손해배상책임을 지우는 법제이다. 우리 대법원은 “사생활의 비밀에 관한 사항을 함부로 타인에게 공개당하지 아니할 법적 이익”을 사생활 권리(프라이버시권)로 인정하고 있을 뿐이다.²²⁾ 이처럼 대법원이 인정하는 사생활권리라는 것도 개인에 관한 모든 정보를 보호하는 것이 아니라 ‘사생활의 비밀에 관한 정보가 외부에 공개되지 않도록 보호’하는 것이다. 비밀정보 그 자체를 보호한다기보다는 그것이 외부에 공개됨으로써 정보주체가 입게 될 인격적 훼손을 방지하고자 하는 데 기본취지가 있다.

이처럼 명예훼손이나 사생활침해의 경우 그 위법성은 ‘한정된 종류의 사실적 개인정보’(사회적 평가를 저하시킬 수 있는 사실 또는 숨기고자 하는 은밀한 사적인 사실)을 여러 사람에게 널리 ‘공표하는 경우’에 비로소 인정된다. 그리고 설령 그러한 사실의 공표가 있다 하더라도 일정한 사유가 있는 때에는 그 위법성이 인정되지 않는다(위법성조각).

요컨대, 명예훼손법과 사생활보호법은 개인정보 중에서도 개인의 사회적 평가를 저하시킬 수 있는 정보나 은밀한 사생활정보에 한정하여 그것도 그러한 정보를 외부로 공표하는 경우에 대해서만 규율하는 법이다. 또 그 경우에도 일정한 사유가 있는 때에는 위법성을 인정하지 않는다. 이러한 법적 한계 내에서 정보주체의 인격적 이익이 보호되고 있다.

그런데 비식별개인정보를 포함하는 모든 개인정보를 정보주체의 인격적 징표라는 이유로 해서, 그리하여 타인이 수집·이용·제공하는 나에 관한 정보는 나의

22) 대법원 1998. 9. 4. 선고 96다11327 판결.

것이라는 과장된 논리로, 만일 정보주체의 동의 없는 개인정보의 수집·이용·제공을 불법으로 금지시킨다거나 당해 정보주체의 인격적 이익을 침해하는 것으로 규정한다면, 이는 인격권에 관한 기존의 법리를 오해한 것일 뿐만 아니라 개인정보의 수집·이용·제공이 가지는 다양한 사회적 이익과 가치를 전혀 고려하지 않은 것이다.²³⁾

또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조는 동의 없는 개인정보의 처리(수집·이용·제공)를 금지하고 이를 위반하는 경우 5년 이하의 징역에 처하고 있다. 그런데 동의 없는 개인정보의 처리를 5년 이하의 징역에 처할만큼 정보통신서비스제공자가 수집·이용·제공하는 모든 개인정보가 그 개인의 사생활비밀에 해당하는 것인가? 형법상의 비밀침해죄(형법 제316조)는 ‘비밀장치에 의해 보존되어 있는 정보’를 그 비밀장치를 깨고 열어 보는 행위를 3년 이하의 징역에 처하고 있다. 그런데 정보통신망법은 정보통신서비스를 제공하고 이용하는 관계에서 정보통신서비스제공자가 이용자의 사소한 개인정보라도 그 이용자의 동의 없이 수집했다면 그 행위를 5년 이하의 징역에 처하고 있다. 또 형법상의 업무상비밀누설죄(형법 제317조)는 의사·변호사 등의 전문가가 의뢰인과의 신뢰관계 속에서 주고받은 의뢰인의 비밀을 제3자에게 누설하는 행위를 3년 이하의 징역에 처하고 있다. 그런데 정보통신망법은 서비스제공이라는 상업적 이용관계에서 생성된 사소한 개인정보라도 그 이용자의 동의 없이 제3자에게 제공했다면 그 행위를 5년 이하의 징역에 처하고 있다. 이러한 상황에서, 일체의 비식별개인정보가 모두 개인정보에 해당하여, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의해 엄격하게 보호된다고 해석하는 것은 법체계의 균형을 무너뜨리는 해석이 될 것이다.²⁴⁾

5. 비교법적 검토²⁵⁾

가. 서론

개인정보의 개념에 관하여 외국의 입법례를 살펴봄으로써 우리나라의 「정보통

23) 성낙인 외, 2008, 725-728면 참조.

24) 성낙인 외, 2008, 745-746면 참조.

25) 성낙인 외, 2008, 701-704면 참조.

신망 이용촉진 및 정보보호 등에 관한 법률」에 규정되어 있는 개인정보의 개념을 해석하는데 시사점을 도출해보기로 한다.

미국, 유럽, 일본의 개인정보보호법제에서는 개인정보(personal information) 외에 추가적으로 개인기록(personal record)과 고유식별자(particular identifying)의 개념을 사용하고 있다. 개인기록이란 개인의 이름, 주민등록번호, 주소, 전화번호 등 개인에 관한 여러 가지 정보들을 묶은 것을 의미한다. 오늘날 개인정보가 처리되는 관행을 보면, 개인에 관한 여러 정보들이 함께 묶어서 처리되고 있으며, 또 그럴 때에 비로소 그 개인정보들이 사회적으로 의미를 가진다. 개인기록은 이러한 개인정보의 묶음을 지칭하는 용어이다. 그리고 그 개인기록 안에는 당해 정보주체를 식별할 수 있게 해주는 고유식별자(예컨대, 이름, 주민등록번호)가 포함되어 있기 마련이다. 이처럼 특정 개인의 신원을 식별할 수 있게 하는 식별자를 고유식별자라고 한다.

우리나라 현행법이 개인기록이나 고유식별자의 개념을 별도로 사용하지 않는데 반해, 미국, 유럽, 일본의 개인정보보호법은 개념을 더욱 세분화하여 사용함으로써 개인정보와 관련된 법률의 입장을 더욱 구체화하고 있다. 미국, 유럽, 일본의 개념 정의를 살펴보면 다음과 같다.

나. 미국

미국의 공공부문 개인정보보호법인 「프라이버시법」(Privacy Act)은 개인정보 외에 개인기록(record), 고유식별자(particular indentifying)의 개념을 사용하고 있다. 프라이버시법에 따르면 개인기록이란 “행정기관이 보유하는 개인에 관한 정보의 개개 항목 또는 그 집합을 말한다. 그 기록에는 그 기록에는 당해 개인의 교육, 금전적 거래(financial transactions), 병력(medical history), 전과(criminal history) 또는 취업경력(employment history)에 관한 정보가 담기지만 이에 한정되지 않는다. 그리고 그 기록에는 당해 개인의 이름, 또는 식별번호나 식별부호 혹은 지문(finger print)·성문(voice print)·사진(photograph)과 같은 당해 개인에게 고유한 식별자(identifying particular)가 포함되어 있어야 한다.”²⁶⁾

이처럼 미국의 「프라이버시법」은 규율의 대상이 되는 “개인기록”(record) 안에 적어도 신원을 확인할 수 있는 식별자가 포함되어 있어야 하고, 그 식별자로 기능할 수 있는 것으로서 1) 이름, 2) 공적으로 부여한 식별번호나 식별부호, 3) 기타 생체식별정보(지문, 성문, 사진)를 명시하고 있다. 그리고 미국의 법은 이러한 개인기록들의 체계적인 묶음, 즉 개인정보데이터베이스를 “개인기록시스템”(system of records)이라고 이름붙이고 있다.

다. 유럽연합

유럽연합의 개인정보보호지침(95/46/EC)도 미국과 유사하게 다음과 같이 규정하고 있다. 즉 “개인기록”(personal data)이라 함은 “신원이 확인된(identified) 또는 신원확인이 가능한(identifiable) 자연인(즉 정보주체)에 관한 일체의 정보를 말하며, 신원확인이 가능한 개인(identifiable person)이라 함은 직접 또는 간접적으로, 특히 신원확인번호(an identification number)나 그의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 동일성(identity)을 고유하게 나타내는 하나 또는 그 이상의 요소를 참조하여 그 신원이 확인될 수 있는 있는 사람을 가리킨다.”

라. 영국

영국의 개인정보보호법(Data Protection Act 1998)도 “신원확인이 가능한 개인 기록”이라는 개념을 사용하고 있다. 즉 “개인기록”(personal data)이라 함은 “신원확인이 가능한 생존하는 개인에 관한 기록(data)으로서, (a) 그 기록으로부터, 또는 (b) 당해 개인정보처리자(data controller)가 보유하고 있거나 또는 앞으로 보유하게 될 다른 정보로부터 신원확인이 가능한 것을 말하며, 이 개인기록에는 당해 개인에 관한 일체의 의견표명 및 당해 개인과 관련해서 개인정보처리자나 그 밖의 다른 사람이 드러낸 일체의 의견이 모두 포함된다.”

26) 5 U.S.C. §522a(a)(4).

마. 일본

일본의 개인정보보호법은 “이 법률에서 개인정보라 함은 생존하는 개인에 관한 정보로서, 당해 정보에 포함되어 있는 성명, 생년월일 그 밖의 기술 등에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조할 수 있고, 그로써 특정의 개인을 식별할 수 있도록 되어 있는 것을 포함한다)을 말한다.”고 규정하고 있다(제2조 제1항).

이는 “당해 정보에 포함되어 있는” 이라는 문언에 비추어 볼 때 정보의 묶음인 개인기록의 개념을 상정하고 있는 것이고, 또 그 기록 안에 특정 개인을 식별할 수 있는 고유식별자가 포함되어야 한다고 규정한 것이다.

6. 소 결

이상의 논의를 종합하면, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 개인정보란, 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(식별개인정보)와, 해당 정보만으로는 특정 개인을 알아볼 수 없는 비식별개인정보라도 이것이 다른 정보와 실제로 결합하여 특정 개인을 식별할 수 있게 된 경우에는 그 정보를 포함한다고 해석하는 것이 타당하다. 이러한 해석은 문리해석, 체계적 해석, 역사적 해석, 목적론적 해석, 비교법적 검토에 의해 누적적으로 지지된다.

현행법의 해석론으로써, 비식별개인정보는 식별개인정보(이름, 주민등록번호 등의 고유식별자)와 결합하여 개인정보의 묶음 안에 결합되어 있을 경우에 한하여, 그럼으로써 특정 개인을 식별할 수 있게 되는 경우에 한하여 개인정보에 해당한다고 할 것이다. 그렇지 않고 식별개인정보와 결합되지 않은 상태에서, 특정 개인을 식별함이 없이 익명화되어 처리되고 있는 경우에는 비식별개인정보가 현행법상 개인정보에 해당하지 않는다고 봄이 타당하다. 결국, 개인을 식별함이 없이 비식별개인정보를 처리하는 경우나, 비식별개인정보를 수집한 뒤 이를 나중에 수집

한 식별개인정보와 결합하는 경우(Retrospective merge)에 대해서는 현행법상 입법의 공백이 있다는 결론에 이르게 된다. 이는 이러한 경우에 대해서도 자율규제 가이드라인이 마련되어 있는 미국의 경우와 대조되는 것이다.

정보주체의 개인정보자기결정권을 보호하기 위해 이러한 입법의 공백을 메우는 작업이 필요하다고 판단된다. 현재와 같은 상황에서는 정보통신망서비스 제공자가 비식별개인정보를 아무런 제한 없이 수집·이용·제공할 수 있고, 또 비식별개인정보를 수집한 뒤 이를 나중에 수집한 식별개인정보와 아무런 제한 없이 결합해서 개인에 대한 프로필을 만들 수 있다. 그러나 이는 정보통신망서비스 제공자의 편의만을 극단적으로 보호하는 것으로서, 그 결과 정보주체의 개인정보자기결정권과 프라이버시가 심각하게 침해될 수 있다.

정보주체가 정보통신망서비스 제공자의 비식별개인정보 이용에 대해 이의를 제기하고 규제를 요구할 수 있는 법적 근거는 헌법상 기본권인 개인정보자기결정권이다. 국가는 정보주체의 개인정보자기결정권을 보호하기 위하여 비식별개인정보의 수집과 활용에 관하여 규제권한을 행사할 수 있고, 정보통신망서비스 제공자는 정보주체가 가지는 개인정보자기결정권을 존중하고 침해하지 않아야 할 의무를 진다. 이러한 점에서 정보주체가 가지는 헌법상 기본권인 개인정보자기결정권에 대한 그 의의, 법적 성질, 효력, 내용 등을 상세하게 살펴볼 필요가 있다. 항목을 나누어 차례대로 살펴보기로 한다.

제4장 개인정보자기결정권의 법적 근거

제1절 서론

오늘날 세계 각국에서는 개인정보를 헌법적 차원에서 보호하기 위해 개인정보자기결정권을 헌법상 기본권으로 승인하고, 이를 보호하기 위한 구체적인 법률을 제정하고 있다. 가령 미국은 1974년 공공영역을 규율하는 프라이버시법(Privacy Act)을 제정하였고 민간영역에서도 부문별로 정보보호에 관한 개별법률을 제정했다. 또한 EU는 1995년에 개인정보보호지침을 제정하고 1997년에 정보통신분야에 적용되는 특별지침을 제정하여 회원국들에게 이를 준수토록 하고 있으며, 영국, 독일, 핀란드, 스페인, 이탈리아 등에서 개인정보보호법 외에도 정보통신분야의 개인정보보호와 관련된 별도의 법률을 제정하여 시행하고 있다.

우리나라에서도 1994년에 「공공기관의 개인정보 보호에 관한 법률」이 제정되고 2001년에 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 제정되는 등 개인정보를 보호하기 위한 일련의 입법이 이루어져왔다. 이러한 법률은 헌법상 개인정보자기결정권을 보호하기 위하여 국가가 기본권보호의무(헌법 제10조 후문)를 이행한 결과라고 할 수 있다.

정보통신망서비스 제공자가 비식별개인정보를 처리하는 것에 대해 정보주체가 이의를 제기하고 규제를 요구할 수 있는 법적 근거가 바로 헌법상 기본권인 개인정보자기결정권이다. 국가가 비식별개인정보의 수집과 활용에 관하여 규제권한을 행사하는 것은 정보주체의 개인정보자기결정권을 보호하기 위한 것이라는 점에서 목적의 정당성이 인정된다. 이 점에서 정보주체가 가지는 헌법상 기본권인 개인정보자기결정권에 대한 그 의의, 법적 성질, 효력, 내용 등을 검토할 필요가 있다. 이하에서 차례대로 살펴보기로 한다.

제2절 개인정보자기결정권의 개관

1. 개인정보자기결정권의 의의

개인정보자기결정권이란 자신에 관한 정보의 공개와 유통을 정보주체가 스스로 결정하고 통제할 수 있는 권리를 말한다. “자신과 관계된 정보의 흐름을 통제하는 권리”, “언제 어떠한 한계 내에서 개인적 생활을 공개할 것인지를 원칙적으로 스스로 결정하는, 개인적 자기결정의 사상에서 나오는 권리”, “자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리” 등으로 정의된다. 개인정보자기결정권이라는 용어 이외에 개인정보자결권, 자기정보통제관리권, 정보자기결정권 등의 다양한 용어가 사용되기도 한다.

2. 개인정보자기결정권의 헌법적 근거

개인정보자기결정권은 헌법에 명시되어 있지 않은 기본권이라는 점에서, 그 헌법적 근거에 관하여 다툼이 있다.

학설로는 헌법 제10조의 인간으로서의 존엄과 가치 및 행복추구권으로부터 도출된다고 보는 견해, 헌법 제17조의 사생활의 비밀과 자유에서 도출된다고 보는 견해, 헌법 제10조 및 제17조를 종합하여 근거를 찾는 견해 등이 대립하고 있다.

헌법재판소는 “개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한 두개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은

이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다.”라고 판시한 바 있다(헌법재판소 2005. 5. 26. 선고 99헌마513결정). 이는 헌법 제37조 제1항을 개인정보자기결정권의 근거로 본 것이라고 할 수 있다.

생각건대 개인정보자기결정권의 근거를 헌법 제17조로 한정하면 개인정보의 범위가 사생활에 관한 정보로 국한되어 개인정보가 불충분하게 보호될 수 있다. 개인정보는 사생활에 관한 정보에 국한되지 않으며 특정 개인을 식별할 수 있는 일체의 정보이기 때문에, 프라이버시보다 외연이 넓은 개념이라 할 수 있다. 또한 개인정보는 개인의 일반적 인격권의 한 내용을 이루는 것으로서, 개인정보가 악용되는 경우 명예훼손 등으로 개인의 인격권이 침해될 수 있다는 점에서 헌법 제10조 역시 헌법상 근거가 된다고 볼 것이다. 나아가 통화기록이나 정치적 견해, 신용정보, 고용정보, 신체장애에 관한 정보 등은 각각 통신의 자유(헌법 제18조), 양심의 자유(제19조), 종교의 자유(제20조), 선거권(제24조), 재산권(제23조), 노동권(제32조, 제33조), 사회보장수급권(제34조) 등과도 관련된다는 점에서 개인정보자기결정권의 헌법적 근거를 어느 한 두 개의 기본권에 국한시키는 것은 어려운 것으로 볼 것이다. 나아가 한편 개인정보자기결정권은 개인의 주관적 공권을 보호하는 기능 뿐만 아니라 정보의 합리적인 유통을 통해 민주주의의 기초를 이루는 기능을 가진다는 점에서, 우리 헌법의 자유민주적 기본질서(근거찾기) 또는 국민주권원리(제1조 제2항)와 민주주의원리(제1조 제2항 등) 등도 그 근거가 된다고 할 수 있다. 이러한 점을 종합하면, 헌법재판소의 판례와 같이 개인정보자기결정권의 근거를 한 두 개에 국한시키지 않고, 헌법에 명시되지 않은 독자적 기본권으로 보는 것이 타당하다고 할 것이다.

< 헌법재판소 2005. 5. 26. 선고 99헌마513결정 >

개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.

개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.

새로운 독자적 기본권으로서의 개인정보자기결정권을 헌법적으로 승인할 필요성이 대두된 것은 다음과 같은 사회적 상황의 변동을 그 배경으로 한다고 할 수 있다.

인류사회는 20세기 후반에 접어들면서 컴퓨터와 통신기술의 비약적인 발전에 힘입어 종전의 산업사회에서 정보사회로 진입하게 되었고, 이에 따른 정보환경의 급격한 변화로 인하여 개인정보의 수집·처리와 관련한 사생활보호라는 새로운 차원의 헌법문제가 초미의 관심사로 제기되었다.

현대에 들어와 사회적 법치국가의 이념 하에 국가기능은 점차 확대되어 왔고, 이에 따라 국가의 급부에 대한 국민의 기대도 급격히 높아지고 있다. 국가가 국민의 기대에 부응하여 복리증진이라는 국가적 과제를 합리적이고 효과적으로 수행하기 위해서는 국가에 의한 개인정보의 수집·처리의 필요성이 증대된다. 오늘날 정보통신기술의 발달은 행정기관의 정보 수집 및 관리 역량을 획기적으로 향상시킴으로써 행정의 효율성과 공정성을 높이는 데 크게 기여하고 있다. 이와 같이 오늘날 국민이 급부행정의 영역에서 보다 안정적이고 공평한 대우를 받기 위해서는 정보기술의 뒷받침이 필연적이라고 할 수 있다.

한편, 현대의 정보통신기술의 발달은 그 그림자도 짙게 드리우고 있다. 특히 컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서 개인정보의 처리와 이용이 시공에 구애됨이 없이 간편하고 신속하게 이루어질 수 있게 되었고, 정보처리의 자동화와 정보파일의 결합을 통하여 여러 기관간의 정보교환이 쉬워짐에 따라 한 기관이 보유하고 있는 개인정보를 모든 기관이 동시에 활용하는 것이 가능하게 되었다. 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체

의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개 될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다.

이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인 하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치라고 할 수 있다.

개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들

과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의 원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것 이므로, 그 헌법적 근거를 굳이 어느 한 두개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다.

3. 개인정보자기결정권의 법적 성질

개인정보자기결정권은 소극적 방어권으로서의 성격과 적극적 청구권의 성격을 아울러 가진다. 즉, 개인정보자기결정권은 자신에 관한 정보를 타인이 동의 없이 수집하고 처리하는 것을 금지시키는 측면에서 고전적인 의미에서의 소극적 방어 권으로서의 성격을 가진다. 한편 타인의 수중에 저장되어 있는 정보를 언제든지 열람하고 오류의 정정을 요구할 수 있는 적극적 청구권으로서의 성격도 동시에 가진다.

4. 개인정보자기결정권의 효력

개인정보자기결정권은 주관적 공권으로서 국가권력을 구속하는 효력을 가진다. 따라서 국가권력은 개인정보자기결정권을 침해할 수 없으며, 정보주체는 개인정보자기결정권을 침해하는 국가작용에 대해 위헌법률심판, 헌법소원심판, 행정소송, 국가배상청구소송 등을 제기하여 다룰 수 있다.

한편 정보통신기술이 발달한 정보화사회에서는 사인들도 자신의 네트워크를 이용하여 타인의 개인정보를 수집, 이용, 처리하는 것이 가능해짐에 따라 사인에 의한 개인정보자기결정권의 침해가 심각한 사회문제로 대두되고 있다. 헌법상 국가의 기본권보호의무에 국가는 사인에 의한 사인의 개인정보자기결정권 침해에 대한 구제를 위한 법률과 정책을 제정하고 집행할 의무를 진다.

5. 개인정보자기결정권의 내용

개인정보자기결정권의 내용은 정보의 처리단계별로 나누어 살펴볼 수 있다.²⁷⁾

개인정보자기결정권

수집에 대한 통제권			보유에 대한 통제권			이용·제공에 대한 통제권	
수집 동의권	설명 청구권	민감정보 수집금지	열람 청구권	정정 청구권	삭제, 차단 청구권	중단 청구권	추가적 동의권

<그림 4-1> 개인정보자기결정권의 내용-자체제작

27) 성낙인 외, 2008, 178-182면 인용.

6. 개인정보자기결정권의 제한

개인정보자기결정권도 절대적으로 제한이 불가능한 기본권은 아니며, 헌법 제37조 제2항의 일반적 법률유보조항에 의해 국가안전보장, 질서유지, 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있다. 개인정보자기결정권을 제한하는 맥락(context)은 다양한데, 제한의 목적에 따라서 다음과 같이 유형을 분류할 수 있다.

- (1) 국가안전보장을 위한 제한 : 반국가적 범죄에 대한 수사 및 재판, 신원조사
- (2) 질서유지를 위한 제한 : 전과조회, 계좌추적, 범죄수사, 성범죄자의 신상공개, 공직자 등의 병역사항이나 재산내역의 공개, 공직선거후보자의 전과공개, 주민등록제도
- (3) 공공복리를 위한 제한 : 국민건강보험의 시행을 위한 의료정보의 조사, 복지혜택의 부여를 위한 소득 등의 조사, 전염병의 예방을 위한 질병조사, 사회생활지표의 작성을 위한 통계조사

7. 개인정보자기결정권의 제한의 한계

개인정보자기결정권은 헌법 제37조 제2항에 의해 국가안전보장, 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있으나, 기본권 제한의 한계로서 과잉제한금지원칙과 본질적 내용 침해금지원칙을 준수해야 한다는 한계가 있다.

헌법재판소에서 개인정보자기결정권을 제한하는 법률에 대해 위헌심사를 한 판례를 살펴보면 다음과 같다.

<<관련된 헌법재판소 판례 조사>>

형의 실효 등에 관한 법률 제8조의2 위헌확인(2009. 10. 29. 2008헌마257 전원재판부)

청구인은 2007년 6월경에 자진거 절취 혐의로 수사기관으로부터 수사를 받은

끝에 ‘혐의없음’의 불기소처분을 받았는데, 이러한 수사결과가 청구인의 수사경력에 관한 전산자료로서 ‘절도-혐의없음’이라는 내용으로 기록되었다. 청구인은 2007년 12월경 위 수사경력에 관한 기록의 존재를 알고 위 기록의 삭제를 요청하였으나, 이는 ‘형의 실효 등에 관한 법률’ 제8조의2에 의하여 불기소처분 결정일로 5년 동안은 기록이 보존되어야 한다는 이유로 거부되었다. 따라서 청구인은 위 법률조항으로 인하여 인격권 등 기본권이 침해받았다는 이유로 법률의 위헌확인을 구하는 헌법소원심판을 청구하였다. 이 헌법소원 청구는 자기관련성, 직접성, 청구기간의 준수 등 적법요건에 있어 흠결이 없기에 본안판결에 들어가게 되었다.

이에 대해 헌법재판소는 ‘수사경력자료’는 사소한 피의사실이라 하더라도 개인이 어떤 범죄혐의로 수사를 받았고 그 처분결과가 어떠한 개인 경력에 관한 정보이고, 이 사건 정보는 개인의 명예와 관련되어 인격주체성을 특징짓는 사항으로서 개인의 동일성을 식별할 수 있게 하는 정보라 할 것이므로, 이 사건 법률조항은 개인정보자기결정권에 대한 제한에 해당한다고 우선 인정하였다.

그러나 ‘혐의없음’에 해당한다고 판단되어도 혐의범죄에 대한 공소시효가 만료되기 전이라면 새로운 증거의 발견이나 새로운 사실관계의 확인 등에 의하여 언제든지 재수사가 이루어질 수 있고, 재수사 끝에 혐의사실이 인정된다면 해당 범죄자를 처벌할 수도 있으므로 수사경력자료는 이와 같은 재수사 상황에 대비한 기초자료로서 보존할 필요성이 있고, 고소인이 해당 범죄사실에 대하여 고소를 반복할 경우에 그 고소를 각하함으로써 범죄수사력의 낭비를 막을 수 있다는 점에서 목적의 정당성이 인정된다. 그리고 이 사건 법률조항이 처리내역에 관한 개인정보를 일정기간 보관한 후 삭제하도록 한 것은 위와 같은 목적을 효율적으로 달성하기 위한 적절한 수단이라고 할 수 있겠다. 다음으로 이 사건 개인정보의 이용범위를 보면 ‘범죄 수사 또는 재판을 위하여 필요한 경우’ 등에 국한되고, 이 사건 개인정보의 누설이나 법령이 규정한 목적 외 취득 및 사용이 엄격히 금지되며 이를 위반한 자는 형사처벌 될 수 있는 점, 개인정보의 법정 보존기간이 합리적 범위 내에 있다고 여겨지는 점 등을 종합적으로 고려하면, 이 사건 법률조항에 의한 것보다 청구인의 개인정보자기결정권을 덜 침해하는 방법이나 수단을 찾아보기 어렵다고 할 것이므로 최소성의 원칙에 위반된다고도 볼 수 없다. 마지막으로 이 사

건 법률조항에 의하여 개인정보를 보관함으로써, 실제적 진실을 구현하기 위한 기초자료를 제공하는 한편 수사력의 낭비를 막고 피의자의 인권을 보호함으로써 달성할 수 있는 공익이 개인정보의 보존으로 입게 되는 정보주체의 불이익에 비하여 더 크다고 볼 수 있다. 따라서 이 사건 법률조항은 과잉금지의 원칙의 위반 여부를 판단함에 있어 모든 요건을 충족하고 있다고 보이므로, 청구인의 개인정보자기결정권을 침해한다고 볼 수는 없다.

의료급여법 시행령 별표 제1호 가목 등 위헌확인(2009. 9. 24. 2007헌마1092 전원재판부)

의료급여 1종 수급권자들인 사건의 청구인은 이 사건의 고시 제3조가 시행되기 전에는 의료급여기관에서 자신이 의료급여 수급권자라는 사실을 알릴 필요 없이 진료나 조제를 받을 수 있었으나, 이 사건 고시 제3조는 의료급여 수급권자로 하여금 자신이 의료급여 수급권자라는 사실은 물론 자신의 병력, 개인신상명세 등 사생활에 관한 사항을 모두 드러내야 의료급여기관으로부터 진료나 조제를 받을 수 있게 하여 청구인들의 사생활의 비밀과 자유를 침해한다고 주장하였다.

심층적으로 살펴보면 의료급여제도는 생활유지능력이 없거나 생활이 어려운 저소득 국민의 의료문제를 국가가 보장하는 공공부조제도로 건강보험과 함께 국민 의료보장의 중요한 수단이 되는 사회보장제도이다. 국민기초생활보장법은 동법에서 정한 급여의 일종으로 ‘의료급여’를 규정하고 이를 특별법인 의료급여법을 통해 규율하도록 하고 있다. 이 사건과 관련하여 고시 제3조에 의하면 각 지방자치단체장은 의료수급권자의 자격을 관리해야하고, 이를 위해 의료급여기관은 ‘의료급여 자격관리시스템’을 통하여 수급권자의 주상병명, 급여일수, 처방전교부기관기호, 처방전교부번호 등을 공단으로 전송해야 한다. 위의 정보들은 수급권자에게 의료급여를 제공하는 기관이 수급권자로부터 수집한 것이거나 그들을 진료하면서 생성된 것으로서, 인격의 내적핵심에 근접하는 의료정보에 해당한다. 따라서 청구인들의 동의 없이 청구인들의 의료정보가 공단 등으로 전송, 보관되는 것은 청구인들의 개인정보자기결정권을 제한하는 것이라고 할 수 있다.

따라서 이러한 제한에 있어서는 헌법 제 37조 제 2항의 과잉금지원칙이 준수되어야 하는데, 우선 위 고시 제 3조는 청구인들이 의료급여를 받을 적절한 수급자인지 여부 및 의료급여의 범위 등을 정확하게 확인하려는데 목적이 있는 것으로 그 목적의 정당성을 인정받을 수 있다. 그렇기 때문에 위의 목적을 달성하기 위하여 공단은 상병명, 급여일수, 처방전교부기관기호, 처방전교부번호 등을 파악하는 것이 필요하다고 할 수 있고, 이 정보를 수집한 의료급여기관이 그것을 공단에 제공하는 것은 적절한 수단이라고 할 수 있다. 나아가서 고시 제3조에 의하여 수집되는 정보의 범위는 지원 및 급여일수의 확인을 위해 필요한 정보로만 제한되어 있고, 정보를 부당한 목적을 위해 사용하지 못하게끔 법규가 마련되어 있으며, 그것을 위반했을 때 징역 또는 벌금형에 처하도록 한 규정 등이 있어 개인의 자기정보결정권이 제한되는데에 따른 피해를 최소화하는 장치가 갖추어져 있고, 수급자격 및 급여액의 정확성을 확보하여 의료급여제도의 원활한 운영을 기한다는 공익이 이로 인하여 제한되는 개인의 사익보다 크다 할 것이므로 법익의 균형성마저도 갖추었다. 따라서 이 사건 고시 제3조는 헌법상 과잉금지원칙에 위배하여 청구인들의 개인정보자기결정권을 침해하는 것이라고 볼 수 없다.

변호사법 제28조의2 위헌확인(2009. 10. 29. 2007헌마667 전원재판부)

사건의 청구인들은 대한변호사협회에 등록을 마친 변호사들이다. 사건의 핵심이 되는 변호사법 제28조2는 2007. 3. 29일에 개정된 법률로서, 이에 따르면 변호사, 법무법인 및 법무조합의 경우 매년 1월말까지 전년도에 처리한 수임사건의 건수 및 수임액을 소속 지방변호사회에 보고하도록 하였고, 그들이 이를 준수하지 않을 경우에는 변호사법상 징계 처분 및 과태료 처분의 대상이 되도록 하였다. 이에 청구인들은 변호사의 영업상 비밀과 같은 수임사건의 건수 및 수임액을 소속 지방변호사회와 같은 제3자에게 보고하도록 하는 것은 영업의 자유, 사생활의 비밀과 자유, 변론권 및 평등권을 침해한다고 주장하면서 그 위헌의 확인을 구하는 헌법소원심판을 청구하였다.

이러한 주장에 대해 헌법재판소의 예전 판례에 따르면 ‘사생활의 비밀’은 국가가

사생활영역을 들여다보는 것에 대한 보호를 제공하는 기본권이며, '사생활의 자유'는 국가가 사생활의 자유로운 형성을 방해하거나 금지하는 것에 대한 보호를 의미한다. 구체적으로 사생활의 비밀과 자유가 보호하는 것은 '개인의 내밀한 내용의 비밀을 유지할 권리, 개인이 자신의 사생활의 불가침을 보장받을 수 있는 권리, 개인의 양심영역이나 성적 영역과 같은 내밀한 영역에 대한 보호, 인격적인 감정세계의 존중을 받을 권리와 정신적인 내면생활이 침해받지 아니할 권리' 등이다. 한편 공적인 영역의 활동은 다른 기본권에 의한 보호는 별론으로 하고, 사생활의 비밀과 자유가 보호하는 것은 아니라고 할 것이다. 그런데 변호사법에 따르면 변호사는 기본적 인권을 옹호하고 사회정의를 실현함을 사명으로 하며, 그 사명에 따라 성실히 직무를 수행하고 사회질서 유지와 법률제도 개선에 노력해야하는 직업으로서 법률가의 능력뿐 아니라 사회적 책임성, 직업적 윤리성 등 직무의 공공성이 어느 직업 활동보다도 특별히 요구된다. 그러한 점들을 감안하여 볼 때, 변호사의 업무와 관련된 수임사건의 건수 및 수임액은 변호사의 내밀한 개인적 영역에 속하는 것이라고 보기는 어렵고, 이 법 조항을 통해 변호사의 사건 수임을 둘러싼 의혹을 해소함과 동시에 지방변호사에 의한 감시절차를 마련하고, 조세행정 전반에 대한 정의를 세우는 등의 목적을 달성함으로써 얻는 공익이 훨씬 크다고 할 수 있으므로 이 사건 법률조항이 청구인들의 사생활의 비밀과 자유를 침해하는 것이라고는 할 수 없다 판단하였다.

소득세법 제165조 제1항 등 위헌확인(2008. 10. 30. 2006헌마1401·1409(병합) 전원재판부)

청구인들은 소득공제제도와 관련하여 환자의 진료비 내역에 관한 정보를 국세청에 제출하도록 의무를 부과하고 있는 소득세법 제165조 제1항, 제4항 및 소득세법 시행령 제216조의3 제2항이 자신들의 개인정보자기결정권, 양심의 자유 등을 침해하여 헌법에 위반된다는 이유로 이 사건 심판을 청구하였다. 청구인들의 주장에 따르면 청구인들의 동의 없이 그들의 진료정보가 국민건강보험공단과 국세청으로 전송되어 보관이 될 때 그것이 불법 유출될 가능성이 있다는 것이다. 실제로

소득공제증빙서류에 기재될 내용은 누가, 언제, 어디서 진료를 받고 얼마를 지불했는가라는 의료비의 지급 및 영수에 관한 것으로 병명이나 구체적인 진료내역과 같은 인격의 내적 핵심에 근접하는 의료정보는 아니다. 그러나 누가, 언제, 어디서 진료를 받고 얼마를 지불했는가라는 사실은 그 자체만으로도 보호되어야 할 사생활의 비밀일 뿐 아니라, 이러한 정보를 통합하면 구체적인 신체적·정신적 결함이나 진료의 내용까지도 유추할 수 있게 되므로, 개인정보자기결정권에 의하여 보호되어야 할 의료정보라고 아니할 수 없다. 따라서 위 진료정보에 대해 본인들의 동의없이 국세청 등으로 전송 및 보관 되는 것은 청구인들의 개인정보자기결정권을 제한하는 것으로서 과잉금지 원칙이 준수되어야 한다.

우선적으로 이 사건 법령조항은 근로소득자의 연말정산을 위한 소득공제증빙자료 제출의 불편을 해소하는 동시에 이에 따른 근로자와 사업자의 시간적, 경제적 비용을 절감하고 부당한 소득공제를 방지하려는 데 목적이 있다. 이 제도의 시행으로 소득공제를 위한 증빙서류제출이 간편해지고 의료비의 부당공제도 방지할 수 있으므로 법령조항의 목적은 정당하다고 할 것이다. 또한 전국의 모든 의료기관의 사업자 등록번호와 기관코드가 외부에 전부 노출되지 않는 이상 청구인들이 우려하는 본인들의 의료정보가 노출되는 일은 일어날 수 없고, 전자서명법상의 공인인증서 등 엄격한 본인확인절차를 통해 제3자 열람의 기회를 근본적으로 제한하고 있으므로 방법에 있어서도 적절한 수단이라고 할 수 있다. 그리고 정보공개를 원치 않는 수진자들의 개인정보는 거부권의 행사로서 보호될 수 있고 또한 개인의 자기정보결정권에 대한 제한이 최소화될 수 있는 제반장치가 충분히 갖추어져 있으므로 기본권의 침해에 있어서도 최소한으로 제한이 되고, 이 사건 법령조항의 목적을 통하여 달성할 수 있는 공익이 개인정보자기결정권 제한으로 인해 축소되는 사익을 능가하는 수준이므로 법익의 균형성 측면에서도 문제가 없다. 따라서 이 사건 법령조항은 헌법상 과잉금지 원칙에 위배하여 청구인들의 개인정보 자기결정권을 침해하였다고 볼 수 없다.

공직선거법 제49조 제10항 등 위헌확인 등(2008. 4. 24. 2006헌마 402·531(병합) 전원재판부)

이 사건 당시의 심판 청구인은 2006년 5월 31일에 실시예정이었던 지역구 시의원에 입후보하기 위하여 한나라당 공천심사위원회에 공천신청을 하였는데 위 공천심사위원회로부터 전과조회기록의 제출을 요청받자 본인의 집행유예 판결을 받은 전과가 기재된 범죄경력회보서를 제출하였다. 그런데 청구인의 전과는 ‘형의 실효 등에 관한 법률’ 제 7조 제 1항에 따라 이미 형이 실효된 것이었다. 청구인은 형의 실효여부와 관계없이 일률적으로 전과기록을 조회, 공개하도록 강제하고 있어 청구인의 평등권, 사생활의 비밀과 자유, 공무담임권을 침해하는 것이라며 이 사건 법률조항에 대하여 헌법소원을 청구하였다.

이러한 청구에 대하여 우선적으로 헌법재판소는 금고 이상의 형의 범죄경력에 실효된 형을 포함시키는 이 사건 법률조항은 개인의 사생활의 비밀과 자유를 제한하는 것으로서, 헌법 제37조 제2항에 따라 기본권제한의 한계원리인 비례의 원칙을 준수하여야 한다고 판시하였다. 실제로 공무원을 선거하는 권리는 국민의 참정권 중에서 가장 중요한 기본적 권리라고 할 것이고, 후보자의 도덕성, 청렴성 및 자질 등 후보자의 객관적이고 사실적인 범죄관련 이력이 국민에게 제공될 필요성 또한 매우 크다. 따라서 실효된 형이라 하지만 금고 이상의 형의 범죄경력을 공개함으로써 국민의 알 권리를 충족하고 공정하고 정당한 선거권 행사를 보장하고자 하는 이 사건 법률조항의 입법목적은 정당하다. 한편으로 후보자의 실효된 전과기록은 비록 민감한 개인정보이기는 하나 그의 사회적 활동에 대한 비판 내지 평가의 한 자료가 되어 그의 공직 후보자로서의 자질과 적격성을 판단하는데 중요한 자료가 될 뿐만 아니라, 선거가 공정하고 제대로 이루어지기 위해선 실효된 형도 포함된 후보자의 전과기록에 관한 정보도 제공될 필요가 있고, 실제로 공직선거에 참여하는 후보자에게는 일반 사인에 비해선 더 큰 부담이 지워질 수밖에 없는 것이기 때문에 방법에 있어서도 적절하다고 할 수 있다. 또한 실효된 형과 관련된 전과기록의 범위와 공개시기 등이 한정되어 있고 이 사건 법률조항으로 인한 입법 목적을 달성하기 위한 덜 제약적인 입법수단이 있다고 보기도 어려우므로 피해 최소성의 원칙에 반한다고 볼 수도 없다. 결론적으로 위의 규정은 선거권자의 알 권리 및 공정하고 정당한 선거권 행사를 보장한다는 월등한 공익을 실현하기 위한 규정으로서, 이러한 공익적 목적을 위하여 공직선거 후보자의 사생활의 비밀과

자유를 한정적으로만 제한하는 것은 법익간의 균형성이 침해된 것이라고 볼 수 없다고 판결하였다.

국민기초생활보장법 제23조 위헌확인(2005. 11. 24. 2005헌마112 전원재판부)

청구인은 거주지 관할 동사무소에 국민기초생활보장법 소정의 급여신청을 한 사람으로서 이에 동사무소는 청구인과 청구인 가족 모두의 금융거래 정보 관련 기록이 기재된 ‘금융거래정보제공동의서’의 제출을 요구하였다. 이에 대하여 청구인은 이러한 금융거래 조사는 청구인의 사생활의 비밀과 자유 및 행복추구권을 침해하여 위헌이라고 주장하면서 심판대상조항의 위헌확인을 구하는 헌법소원을 제기하였다. 이 규칙조항에 따라 요구된 금융거래정보를 제출하지 않는 경우에는 급여신청이 각하될 수 있으므로 이 규칙조항은 금융거래정보의 제공을 상당한 정도로 강제하는 효과를 갖게 되고 이 범위 하에서 개인정보의 자기결정권 또한 제한하게 된다.

하지만 이 규칙조항은 자신의 소득이나 재산 등으로 최저생활이 가능한 사람까지도 국민기초생활보장법의 수급자가 되는 것을 방지하고 국가의 도움이 정말 필요한 사람에게 보장급여가 지급되도록, 급여신청자의 수급자격 및 급여액 결정을 객관적이고 공정하게 관장하려는 데 그 목적이 있는 것이라 정당성이 인정된다. 보장법상의 급여를 받을 수 있는 자는 소득인정액이 최저생계비 이하인 자이므로 필요한 급여액의 정도를 파악하기 위해선 반드시 그 소득 및 재산을 파악하여야 하는데 금융거래정보의 파악은 이를 위한 적절한 수단이고, 이 사건 규칙조항에 의하여 수집되는 개인정보는 최소한으로 제한이 되어 있으며 이를 수집하는 자가 다른 용도로 사용하는 경우에는 3년 이하의 징역과 1천만원 이하의 벌금에 처하여 지게 되므로 개인정보 자기결정권 제한에 따르는 피해를 최소화하기 위한 장치가 마련되어 있으며, 그러한 제한으로 인해 입게되는 정보주체의 불이익이 수급자격 및 급여액의 객관성과 공정성을 확보한다는 공익에 비하여 더 크다고 볼 수 없으므로 이 규칙조항은 개인정보 자기결정권을 과도하게 제한하여 침해하는 것이라고는 볼 수 없다.

**공직자등의병역사항신고및공개에관한법률 제3조 등 위헌확인(2007. 5. 31.
2005헌마1139, 전원재판부)**

청구인은 징병검사에서 한쪽 눈 실명으로 병역면제 처분을 받았고, 현재 국회 정책연구위원으로 근무하고 있는 공무원으로서, ‘공직자등의 병역사항 신고 및 공개에 관한 법률’에 따라 병역사항을 신고해야하게 되었는데, 같은 법 제3조에 의하여 병역처분을 할 때의 질병명을 신고하여야 했다. 청구인은 질병명까지 신고, 공개토록 하고 있는 위 법률조항에 대하여 자신의 사생활의 비밀과 자유, 직업선택의 자유 등의 기본권을 침해한다는 명목으로 위헌확인을 구하는 헌법소원심판을 청구하였다.

원래 이러한 병역공개제도는 ‘부정한 병역면탈의 방지’와 ‘병역의무의 자진이행에 기여’라는 목적을 달성하기 위하여 입법된 것인데 위와 같은 입법목적을 달성하기 위해서는 병역사항을 신고하게 하는 것뿐만이 아니라 적절한 방법으로 이를 공개하는 것이 필요하다고도 볼 수 있다. 하지만 사람의 육체적·정신적 상태나 건강에 관한 정보는 인간의 존엄성이나 인격의 내적 핵심을 이루는 요소로서 이처럼 민감한 개인정보의 일방적 공개의 범위와 방법을 정하는데 있어서는 사생활의 비밀과 자유를 보장하는 헌법 제 17조의 의미와 작용을 충분히 감안하여야 한다. 그러한 면에서 판단해보건대, 이 사건 법률조항에 의하여 그 공개가 강제되는 질병명을 내밀한 사적 영역에 근접하는 민감한 개인정보이다. 질병이라는 것은 병역처분, 특히 병역면제 여부를 가리는데 있어서는 본질적인 요소이긴 하지만 그것은 개인이 선택 혹은 조정할 수 있는 사항이 아닌데, 이 사건 법률조항은 질병명 공개의 범위와 방법을 정함에 있어서 위와 같은 사생활의 비밀과 자유라는 기본권이 지니는 의미와 작용을 제대로 고려하지 않고, 무차별적으로 공정한 판정에 따른 정당한 면제처분을 받았던 공무원들의 질병명마저 공개하게끔 요구하였다. 또한 법률조항에 따라 4급 이상의 공무원들은 누구나 민감한 개인정보인 질병명을 공개해야했는데, 이는 지나치게 포괄적이고 광범위한 것으로서 4급 공무원이라 할지라도 어떤 주요 정책이나 기획의 직접적, 최종적인 결정권을 가진다고 할 수 없고 평범한 한 명의 직업인에 불과한 경우도 많기에 이들의 정보를 공개하는 것이

어떠한 공익을 달성하기에는 적합하지 않은 수단이라고 해야 할 것이다. 따라서 헌법재판소는 이러한 이유를 들어 이 법률조항의 위헌의 소지가 있지만 단순위헌결정을 하는 것은 적절하지 않다고 판단하여 빠른 시일 내에 개선입법을 촉구하고 그대까지는 이 법률조항의 계속적용을 명하는 헌법불합치 판정을 내렸다.

개인정보수집 등 위헌확인(2005. 7. 21. 2003헌마282·425(병합) 전원재판부)

청구인은 초등학교 1학년에 재학 중인 학생과 그의 아버지, 그리고 다른 청구인은 서울특별시 교육청 산하에 한 고등학교를 졸업한 자이다. 청구인들은 교육인적자원부장관과 서울특별시 교육감이 교육정보시스템(NEIS-National Education Information System)을 통하여 청구인 A의 학적, 학생생활, 성적, 건강 및 의료 등에 관한 정보, 청구인 B의 성명, 주민등록번호, 직업, 최종학력, 생년월일, 가족 상호아에 관한 정보, 청구인 C의 성명, 주민등록번호, 생년월일, 졸업학교명, 졸업 연월일에 관한 정보를 수집하고 이에 대한 정보파일을 보유하고 있는바, 그것이 청구인들의 행복추구권 사생활의 비밀과 자유 등의 기본권을 침해하는 것이라고 주장하면서 헌법소원심판을 청구하였다.

헌법재판소는 청구인 A와 청구인 B의 헌법소원 청구에 대하여 기본권침해의 자기관련성이 없다고 판단하여 부적법한 심판 청구라 하여 청구인 C의 심판청구에 대해서만 본안판단을 내리게 되었다. 피청구인들이 청구인 C의 개인정보를 개인정보파일로 작성하여 보유하는 근거는 개인정보법 제5조에서 찾을 수 있는데, 피청구인들은 졸업생 관련 제 증명의 발급이라는 소관 민원업무를 효율적으로 수행함에 필요하다고 보아 기존의 수기로 된 졸업대장의 자료를 토대로 위 청구인의 개인정보를 담고 있는 개인정보파일을 작성하여 유지, 관리하고 있는 것이다. 그런데 성명, 생년월일은 최소한의 개인식별정보로서 모든 행정업무 처리에 불가결한 기초정보에 불과하고, 졸업일자도 개인에 관한 의미있는 정보이기는 하지만 개인의 인격에 밀접히 연관된 민감한 정보라고는 보기는 어렵다고 하였다. 따라서 국민의 편의를 도모한다는 점과 수권법률의 명확성이 특별히 강하게 요구된다는 할 수 없다는 점을 고려해보건대, 피청구인들의 보유행위가 이루어졌다고 하되

라도 법률유보원칙에 위배된다고 단정할 수 없다고 판단하였다.

또한 비례성원칙으로 판단해보아도 NEIS는 교육행정의 생산성 투명성 확보, 교원업무의 경감, 인터넷을 통하여 학부모에게 정보 제공 제 증명서 발급 등의 민원 서비스를 제공하고자 하는 목적으로 도입된 것이라 그 목적의 정당성이 인정되며, 피청구인들이 보유하고 있는 정보들이 그 자체로 개인의 존엄과 인격권에 심대한 영향을 미칠 수 있는 민감한 정보라고는 보기 어려워서 청구인 C의 심판청구는 이유없으므로 기각하고, 공익적인 목적을 위해 최소한의 정보만을 보유하는 행위는 개인정보 자기결정권을 침해하는 것이라고는 할 수 없다.

청소년의성보호에관한법률 제20조 제2항 제1호 등 위헌제청(2003. 6. 26. 2002헌가14 전원재판부)

위헌여부심판제청인은 2000. 7. 1. 청소년에게 6만원을 제공하고 1회 성교행위를 하여 청소년의성보호에관한법률 제5조를 위반하였다는 혐의로 2000. 8. 전주지방법원에서 벌금 500만원을 선고받았고, 청소년보호위원회는 2001. 5. 위 법률 제20조에 근거하여 제청신청인의 성명, 연령, 생년월일, 직업, 주소 등과 범죄사실의 요지를 관보에 게재하고 같은 내용을 청소년보호위원회의 인터넷 홈페이지에 6개월간, 정부중앙청사 및 특별시, 광역시, 도의 본청 게시판에 1개월간 게시하기로 하는 결정을 하였다. 이에 제청신청인은 신상등기공개처분의 취소를 구하는 소를 제기한 후, 위 법률 제20조에 대한 위헌여부심판제청을 신청하였는데, 법원이 이중 일부의 신청만을 받아들여 2002. 7. 26. 헌법재판소에 위헌여부심판을 제청하였다. 제청신청인의 의견에 의하면 범죄사실의 요지는 사생활의 비밀에 해당하고 이것이 의사에 반하여 외부에 공표될 경우 청소년 성매수자로서는 인격적인 수모를 느끼게 된다. 따라서 현행의 신상공개제도는 청소년 성매수자의 인격권 내지 사생활의 비밀을 과도하게 침해하는 것이라고 주장하였다.

원래 청소년 성매수자 신상공개제도는 미국의 메간법을 참조하여, 그러한 형태의 범죄를 예방하기 위한 수단으로 제도의 목적을 가지고 있고, 제도의 의도로서 범죄인의 신상을 공개하는 것이 범죄예방을 위한 효과적인 방법이라는 판단에서

입법되어 여태까지 시행되어 온 것이다. 실제로 인터넷과 같은 매체의 급속한 발달과 맞물려 도덕성의 심각한 해이 현상이 일어나게 되었고, 더 이상 성인이나 청소년들의 도덕성에만 그 개선을 기대할 수 없는 지경에 이르렀기에 우리 사회의 성문화에 대한 최소한의 도덕성을 지키는 한편 헌법 제 37조 제 2항에서 명시된 공공복리를 위해 이러한 입법은 꼭 필요한 것으로서 정당성이 인정된다고 할 수 있다. 그리고 신상공개제도를 통해서 일반 성인들에게 미성년자 성매수자가 되지 않도록 하는 위하적 내지 예방적 효과를 줄 수 있을 뿐만 아니라, 종래의 형벌이나 보안처분만으로는 아동과 청소년의 소중한 성을 보호하기 위해 불충분했던 점을 보충할 수 있고 청소년 대상 성범죄의 충동을 억제하게 하는 효과도 있으므로 수단의 적절성도 인정이 된다. 이 목적달성을 위해선 누구나 쉽게 접근할 수 있는 공개수단이 선택될 필요가 있고, 또한 신상공개정보제도가 달리 다른 입법수단이 있음에도 불구하고 해당 범죄인들의 기본권을 더 제한하는 것이라 단정할 수 없고 어떠한 것이 보다 덜 침해적인지를 판단하기 어려운 상황에서 어떠한 수단을 선택할 것인지는 입법자의 형성의 권한이라고 할 것이다. 결론적으로는 신상공개제도를 통해 현존하는 성폭력위험으로부터 사회공동체를 지키자는 인식을 제고하는 한편, 가장 중요한 공익 중의 하나인 ‘청소년의 성보호’를 달성할 수 있고, 청소년 대상 성범죄자에 있어서는 인격권과 사생활의 비밀도 그것이 본직적인 부분이 아닌 이상 다른 범죄자에 비하여 보다 넓게 제한될 여지가 있다고 볼 것이므로, 이 사건 법률조항이 해당 범죄인들의 일반적 인격권, 사생활의 비밀의 자유를 과잉금지 원칙에 위배하여 침해한 것이라고 볼 수는 없다.

주민등록법 제17조의8 등 위헌확인 등(2005. 5. 26. 99헌마513, 2004헌마190 (병합) 전원재판부)

청구인들은 이미 주민등록증을 발급받은 사람들로서, 사회운동단체에 소속되어 있고, 주민등록증 일체갱신을 계기로 지문날인 반대운동을 하고 있는 사람들이다. 위 청구인들은 주민등록증을 발급받을 당시 자신들이 주민등록증 발급신청서에 날인함으로써 만들어진 열 손가락의 지문정보를 피청구인 경찰청장이 보관, 전산

화하고 이를 범죄수사목적에 이용하는 공권력행사로 인하여 자신들의 인간의 존엄과 가치, 행복추구권, 인격권, 신체의 자유, 사생활의 비밀과 자유, 개인정보자기결정권 등을 침해받았다고 주장하면서 그 위헌확인을 구하는 이 사건 헌법소원심판을 청구하였다. 청구인들이 주장하듯이 개인의 고유성, 동일성을 나타내는 지문은 그 정보주체를 타인으로부터 식별가능하게 하는 개인정보이므로, 시장, 군수 또는 구청장이 개인의 지문정보를 수집하고, 경찰청장이 이를 보관, 전산화하여 범죄수사목적에 이용하는 것은 모두 개인정보자기결정권을 제한하는 조치들이다. 따라서 개인정보자기결정권에 제한에는 법률적인 근거가 필요하다.

지문은 그 자체만으로는 타인의 평가로부터 단절된 중립적인 정보이고, 일반인이 아닌 전문적인 감식능력이 있는 사람만이 그 정보주체를 확인할 수 있는 것이고, 정보주체로부터 정보수집자에게로 전달되는 과정에서 정보의 내용이 실제 내용과 다르게 왜곡될 염려가 없는 객관적인 정보이다. 이와같은 특성들로 인하여 지문정보는 개인의 자기정보 결정권을 제약하는 요소로 작용할 여지가 일반적으로 작은 것이 사실이다. 지문은 가장 정확하고 효율적인 신원확인 수단으로서 범죄현장에서 채취한 지문과의 대조, 대형사건사고가 발생한 경우의 신원확인, 타인의 인적사항 도용방지 등의 목적으로 사용되고 있는 바 결국 모두 개인의 신원확인이라는 점으로 지문정보의 활용은 귀결된다. 이러한 지문정보를 보관하는 행위는 주민등록법 제17조의8 제2항 본문, 제17조의10 제 1항 등에 근거하는 것으로 볼 수 있어, 법률유보의 원칙에 위배되는 것이라고 할 수 없다.

과잉금지 원칙에 위배되는지를 살펴보면 모든 국민의 열 손가락 지문정보를 수집하고 이를 보관, 전산화하는 것은 신원확인의 정확성 내지 완벽성을 제고하기 위한 목적을 달성하기 위해 효과적이고 적절한 방법의 하나가 될 수 있음은 물론이요, 정확성, 간편성, 효율성 등의 종합적인 측면에서 이와 비견할만한 것이 찾아보기 어려운 실정이다. 또한 다른 신원확인 수단으로서 유전자, 홍채, 치아 등이 거론되고 있으나 이러한 정보를 수집하는 것은 오히려 과도한 인권침해의 우려가 있으므로 지문 수집이 피해의 최소성 원칙에도 충족하고 있으며, 대형사건사고나 변사자가 발생한 경우의 신원확인, 타인의 인적사항 도용 방지 등 각종 신원확인의 목적을 위하여 이용함으로써 달성할 수 있게 되는 공익이 그로 인한 정보주체

의 불이익에 비하여 더 크다고 보아야 할 것이기 때문에, 이 사건 지문날인제도에 의한 개인정보자기결정권의 제한은 과잉금지의 원칙의 위배 여부를 판단함에 있어 고려되어야 할 목적의 정당성, 방법의 적정성, 피해의 최소성 및 법익의 균형성 등 모든 요건을 충족하고 있다고 보이므로 개인정보자기결정권을 침해하였다고 볼 수 없다.

8. 사권(私權)으로서의 개인정보자기결정권²⁸⁾

이상에서 설명한 ‘개인정보자기결정권’은 일단 국가에 대한 기본권이라는 점에서 공권(公權)에 해당한다. 그렇다면 이러한 권리는 사인 간에도 그대로 주장할 수 있는가? 다양한 종류의 온라인 행태정보의 보호에 관한 권리의무는 개인기업과 이용자간의 관계인 경우가 많기 때문에 아주 중요한 질문이 될 것이다.

그렇다고 보아야 한다. 개인정보자기결정권과 밀접한 관련이 있는 프라이버시권도 개인간의 법률관계에 효력을 가진다고 해석하는 데에 이견이 없다. 개인정보보호에 관하여서도 마찬가지로 해석할 수 있다. 우선 관련 법령들의 내용을 살펴보면, 개인정보보호의무가 사인간에도 존재한다는 점을 전제하고 있다. 공공기관법은 원칙적으로 국가 내지 지방자치단체와 국민 사이의 관계를 규율하고 있지만, 제22조에서는 “공공기관외의 개인 또는 단체는 컴퓨터등을 사용하여 개인정보를 처리함에 있어 공공기관의 예에 준하여 개인정보의 보호를 위한 조치를 강구하여야 하며…”라고 규정한다. 정보통신망법 제22조 이하, 암관리법 제12조, 결혼중개업의 관리에 관한 법률 제13조, 소비자기본법 제15조, 전자서명법 제24조, 유비쿼터스도시의 건설 등에 관한 법률 제21조는 모두 사인 간의 개인정보보호관계에 관하여 규정한다. 아직 사인간의 개인정보보호의무에 관한 포괄적인 조항은 없지만, 위 조항들에 내재하는 전체적 법질서의 정신으로부터 이러한 의무를 도출할 수 있다. 그러므로 개인정보를 수집, 관리, 이용하는 주체는 법률의 명문 규정이 있는 경우에는 그 규정에 의하여, 그렇지 않는 경우에도 위와 같은 규정들을 종합하면 도출되는 법의 일반원칙 또는 조리(條理)에 의하여 타인의 개인정보를 보호할 법적 주

28) 정상조·권영준 공저, 個人情報의 보호와 民事的 救濟, 법조 58권3호 통권630호 (2009.3.) 14면.

의의무를 부담한다.

현실적으로 보더라도 개인정보자기결정권이 침해되었다는 이유로 사인 간에 민사소송이 진행되는 사례가 다수 있다. 법원 역시 위와 같은 권리가 사인간에도 관철될 수 있다는 점을 전제로 판결을 선고하고 있다.

제3절 온라인 맞춤형 광고에 따른 기본권의 충돌

1. 서론

비식별 개인정보가 정보통신망 서비스 제공자에 의하여 수집되고 처리되는 데 있어서 정보주체가 이의를 제기할 수 있는 법적인 근거가 될 수 있는 것이 바로 헌법상의 기본권인 개인정보 자기결정권이다. 결국 개인정보자기결정권이란 재산에 관한 정보의 공개와 유통을 정보주체가 스스로 결정하고 통제할 수 있는 권리로서, 헌법재판소 판례에 따르면 이 기본권은 헌법에 명시되지 않은 독자적인 기본권이다. 개인정보 자기결정권은 소극적 방어권으로서의 성격과 적극적 청구권으로서의 성격을 두루 갖추고 있으며, 이로 인하여 국가는 국민의 권리를 보호하기 위해 필요한 법률과 정책을 제정하고 집행해야만 한다. 하지만 이 기본권도 절대적으로 보장될 수만은 없다. 헌법 제37조 제2항의 일반적 법률유보조항에 의하여 개인정보 자기결정권은 국가안전보장, 질서유지, 공공복리 등을 위하여 필요한 경우에 법률로써 제한이 될 수 있고, 그 뿐만 아니라 앞에서 살펴본 판례들을 통해서도 개인정보 자기결정권이 제한된다고 하더라도 침해되는 것이라고는 볼 수 없는 사례가 존재한다는 사실을 우리는 알 수 있다. 더 나아가서 이제는 개인정보자기결정권을 보호하는 과정에 있어서 헌법상으로 보장된 다른 기본권과 충돌이 있는 경우에, 그것을 어떠한 방법을 통해 보호해야 다른 기본권을 배척하지 않으면서도 헌법에 합치될 수 있는지를 살펴보는 것이 중요한 쟁점이라고 할 수 있다.

기업들은 보다 많은 소비자들을 고객으로 만들기 위하여 항상 새로운 판매 전략을 시도하는 한편, 그러한 노력의 일환으로써 소비자들의 정보를 수집하여 그들

이 원하는 바가 무엇인지를 파악하고 효율적인 마케팅의 수단으로 사용해왔다. 그런데 현대 시대에는 정보통신 기술의 비약적인 발달로 인하여 기업들이 소비자의 이름, 주민등록번호, 주소 등 특정 개인을 식별할 수 있는 식별개인정보뿐만이 아니라 소비자의 사이트 접속기록, 서비스 이용기록, 관심분야, 구매내역, 결제기록, IP 주소, 현 위치 등 소비자의 행태, 성향 혹은 위치와 관련된 정보들까지도 수집, 가공할 수 있게 되어, 그것들을 소비자를 위한 맞춤형 광고를 하는 데에 사용할 수 있는 현실적 제반조건이 형성되었다. 소비자의 행태, 성향, 위치 정보 등은 그 자체만으로는 특정 개인을 식별할 수 없는 탓에, 비식별개인정보라고 할 수 있다. 하지만 이들이 식별 가능한 다른 정보들과 결합되었을 때에는 얼마든지 개인을 특정할 수 있는 개인정보가 될 수 있으므로, 그러한 정보를 기업들이 사용하는 데 있어서는 정보의 주체에게 헌법적으로 보장된 권리인 '개인정보자기결정권'에 대한 고려가 필수적으로 요구된다고 할 수 있다. 소비자들은 당연히 개인정보자기결정권에 의하여 자신에 관한 정보의 공개와 유통을 스스로 결정하고 통제할 수 있는 권리를 가지기 때문이고, 기업은 이를 침해하면서까지 마케팅을 할 수는 없기 때문이다. 하지만 소비자의 개인정보에 관한 자기 통제권과 프라이버시에 관한 권리가 헌법적으로 보장되는 권리라는 이유만으로, 기업들의 존재목적인 수익추구에 필수적으로 수반되는 활동인 광고표현을 함부로 금지하는 것을 정당화할 수는 없을 것이다. 광고주체의 입장에서라도 그들이 수집한 소비자의 행태, 성향 등의 정보가 식별가능정보와 결합되어 소비자의 개인정보자기결정권을 침해하지 않는 선에서는 비식별 개인정보를 활용한 맞춤형 광고에 대한 광고표현의 자유, 영업의 자유, 재산권, 일반적 행동자유권 등을 주장할 수 있기 때문이다. 그런데 이 가운데 소비자형 온라인 맞춤형 광고와 가장 밀접한 관련이 있고, 실제로 광고 규제에 의해 가장 많은 제한을 받는 기본권은 광고표현의 자유라 할 것이다. 따라서 지금은 소비자의 '개인정보자기결정권'과 광고 주체의 '광고표현의 자유' 이 두 가지의 기본권이 충돌하고 있는 상황에서 어떠한 해결책을 찾아야할 지가 중요한 문제로 대두된 시점이라고 할 수 있다.

2. 광고표현의 자유

기본권의 충돌을 논하기 위해선 우선 광고주체가 주장하는 ‘광고표현의 자유’가 실제로 헌법으로 보장되는 권리인지가 가장 중요하다고 할 수 있다. 외견상으로 주장되는 기본권이라고 할지라도 본질상으로 기본권에 해당하지 않는다거나 기본권의 이름으로 보호될 수 없는 경우라 한다면, 처음부터 기본권의 충돌이라는 말 자체가 성립할 수 없기 때문이다. 이것을 살피기 위해선 광고주체들이 주장하는 ‘광고표현의 자유’가 대한민국 헌법 어디에서 규정되고 있는 것인지를 알아볼 필요가 있다. 이를 위해 우선 대한민국 헌법 제 21조에서 말하고 있는 ‘표현의 자유’를 살펴보기로 한다.

대한민국 헌법 제21조

- ① 모든 국민은 언론·출판의 자유와 집회·결사의 자유를 가진다.
- ② 언론·출판에 대한 허가나 검열과 집회·결사에 대한 허가는 인정되지 아니한다.
- ③ 통신·방송의 시설기준과 신문의 기능을 보장하기 위하여 필요한 사항은 법률로 정한다.
- ④ 언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니된다. 언론·출판이 타인의 명예나 권리를 침해한 때에는 피해자는 이에 대한 피해의 배상을 청구할 수 있다.

광고표현의 자유를 대한민국 헌법 제 21조가 보장하고 있는 자유에 속하는지에 대해선 의견이 나누어지기도 한다. 우선 광고를 표현의 자유로 보지 않는 조영황 변호사의 견해에 따르면²⁹⁾,

‘표현의 자유는 정신활동의 자유이다. 여기의 정신활동이란 직접적으로 인격발현을 위한 것이어야 한다. 따라서 정신활동의 자유라고 볼 수 없는 영리적인 광고 등은 표현의 자유로 파악할 수는 없고 영업의 자유로 이해해야 할 것이다. 표현의 자유는 표현수단을 물적으로 보장하는 것은 아니다. 따라서 표현수단인 옥외광고물이

29) 이구현, 광고와 표현의 자유, 언론과 법, 한국언론법학회, Vol 4, No. 1(2005), p.199.

미관을 해치는 경우에는 보장할 수 없다는 법리적인 해석이다. 표현행위에는 적극적 및 소극적 표현의 양작용을 포함한다. 그러므로 표현의 자유는 소극적으로는 일정한 내용표현을 강제당하지 아니할 자유권이며 적극적으로는 자기의 특수적 의사를 외부로 표현하는 자유권을 말한다. 그리고 표현의 내용은 주로 사상 또는 의견을 말한다.’

그러나 헌법재판소에 의하면 광고행위 또한 현대 자본주의 사회의 ‘필수불가결한 제도’로서 단순히 상업적인 상품이나 서비스에 관한 사실을 알리는 경우라 할지라도 그 내용이 공익을 포함하는 때에는 헌법 제 21조의 표현의 자유에 의하여 보호된다는 원칙을 일련의 판례(96헌바2, 99헌마143, 2000헌마764, 2003헌가3 등 참조)를 통하여 천명하였다. 그 판례들을 통해 우리는 헌법재판소가 과잉금지원칙, 명확성의 원칙, 사전허가금지 원칙, 그리고 포괄위임금지 원칙 등 4가지의 검증절차를 이용하여, 광고를 사상, 지식, 정보 등을 표현 전파하는 매개로서 국민의 ‘알권리의 정보원으로서’의 역할을 인정했다고 알 수 있다.³⁰⁾ 따라서 이제는 광고주체에게 허용된 ‘광고표현의 자유’가 헌법적으로 인정된 기본권이라는 사실을 알 수 있기에 기본권의 충돌에 대해서 논할 수 있을 것이다.

3. 기본권 충돌의 해결방안

가. 기본권충돌의 의의

기본권간의 충돌이란 원칙적으로 서로 다른 둘 이상의 기본권의 주체들 사이에 있어서 서로 충돌하는 각자의 기본권을 주장, 행사하기 위하여 국가에 대하여 각기 자기의 기본권을 주장하는 경우에 그 기본권들 사이에 발생하는 상황을 말한다.³¹⁾ 기본권의 충돌은 한 기본권의 주체가 자신의 기본권을 행사하는 경우, 다른 기본권의 주체가 자신이 보유하고 있는 기본권에 제한이나 침해로 입을 수 있다는 점

30) 엄기열, 표현의 자유와 소비자의 알권리로서의 광고- 광고 및 비교광고와 관련된 규제의 변화 및 판례분석, 언론과 법, 한국언론법학회, Vol.6, No.2(2007), pp.332-341.

31) 정종섭, 전제서, p.345.

에서 그 특징이 있다. 실제로 사인은 다른 사인에 대하여 자기의 기본권을 직접적으로 주장할 수는 없기 때문에 기본권의 행사에 있어 실제 기본권들이 충돌하는 상황은 발생하지 않고, 주로 기본권의 상충은 국가에 대하여 기본권을 주장하는 경우, 혹은 입법, 행정, 재판을 함에 있어서 관련 이익을 조정하는 경우에 발생하게 된다.

나. 기본권충돌의 해결방안

1) 학설

가) 입법 형성의 자유 이론

기본권이 충돌하는 경우 그 문제를 해결하는 방법에 대하여 여러 가지 학설이 제시되곤 하는데 그 첫 번째로 나오는 것은 입법 형성의 자유이론이다. 이에 의하면 기본권의 충돌을 해결하는 방법에 대해 헌법이 명시적으로 정하지 않은 경우라고 한다면 헌법재판소나 법원은 이를 헌법해석을 통해서 해결하려고 하면 안 되고, 철저히 의회의 입법 활동을 통해 해결해야 한다고 한다. 그러나 기본권의 충돌 문제는 성질상으로 헌법과 관련된 문제이기 때문에 헌법의 문제를 법률로서 다루는 것은 옳지 않다는 것과 함께, 모든 충돌현상들이 입법으로 정형화되지도 않는다는 크나큰 비판에 직면하게 된다.

나) 기본권의 서열 이론

이 학설에 의하면 헌법이 보장하는 기본권 사이에는 가치나 중요도에 있어서 서열이 존재한다고 보고, 기본권들이 서로 충돌하는 상황이 발생한다면 충돌하는 기본권들을 이들 서열에 비추어 보다 중요하다고 생각되는 높은 서열의 기본권을 우선하여 보호하는 쪽으로 해결해야 한다고 한다. 그러나 헌법상의 기본권들에 모두 차등을 두어 서열화하는 것은 어려울 뿐만 아니라 불가능한 것이라는 비판이 제기된다.

다) 법익형량이론

두 개의 기본권이 충돌하는 일이 발생하면 그들을 서로 비교형량하여 보다 큰 법익을 보장하는 상위의 기본권을 하위의 기본권에 우선 시켜 해결해야 한다는 학설이 법익형량이론이다. 법익형량이론은 기본권 자체에서보다는 기본권이 보호하고 있는 법익에서 우열의 존재를 인정하여 그것들을 서열화할 수 있고 법익의 서열을 통하여 기본권을 비교형량할 수 있다는 견해이다. 하지만 큰 법익만 보호하고 상대적으로 작은 법익을 보호하지 않고 무시한다는 것은 정당하지 못하고, 기본권 충돌상황에 있어서 매번 법익형량의 객관적인 기준을 찾는다는 것이 어렵다는 비판을 받게 된다.

라) 규범조화이론

법익형량이론은 어느 하나의 기본권을 보호하고 다른 기본권은 배제되는 양자택일의 방법이라고 할 수 있다. 하지만 규범조화이론에 따르면 이러한 방법을 취하지 않고 충돌하는 기본권들을 가능한 한 모두 보호할 수 있는 최적화된 균형점을 찾고자 하며, 헌법의 통일성이라는 관점에서 설사 기본권 사이에 우열이 있다고 할지라도 서열에 관계없이 현실에서 가능한 한 타협점을 찾아 실현하고자 한다. 이에 의하면 첫째로 충돌하는 기본권들에 비례적인 제한을 가하여 모든 기본권이 양립될 수 있는지를 찾아보고(비례적 제한의 원칙), 그것이 불가능하다고 판단되면 대안을 모색하며(대안모색의 원칙), 마지막으로 대안도 발견할 수 없는 상황이라면 한 개의 기본권을 선택하여 불가피하게 후퇴는 시키되, 이러한 후퇴가 기본권을 과도하게 제한해서는 안 된다(과잉금지의 원칙).

2) 판례

대한민국 헌법재판소나 대법원은 기본권의 충돌이라는 문제를 해결하는 데 있어 규범조화적인 방법을 사용하기도 하고, 기본권 서열이론을 채택하기도 하였으

며, 법익형량의 방법을 사용하기도 한다. 또한 이 방법들을 복합적으로 고려하기도 하는데 각 판례의 입장을 살펴보기로 하자.

<헌법재판소 1991. 9. 16 - 89헌마165- 규범조화적인 방법을 사용한 판례>

두 기본권이 서로 충돌하는 경우에는 헌법의 통일성을 유지하기 위하여 상충하는 기본권 모두가 최대한으로 그 기능과 효력을 나타낼 수 있도록 하는 조화로운 방법이 모색되어야 할 것이고 (중략) 반론권은 신속한 권리구제의 필요성에서 보도가 행해진 시간과 근접하여 그 사실 주장을 반박할 기회를 주는 점을 특색으로 하는 것이므로 반론의 제도와 언론의 자유의 관계는 단순히 제도의 평면적 비교나 판단보다 기본권간의 조화라는 전체적인 관점에서 평가되어야 한다. 현행 정정보도청구권제도는 그 명칭에 불구하고 피해자의 반론게재청구권으로 해석되고 이는 언론의 자유와는 비록 서로 충돌되는 면이 없지 아니하나 전체적으로는 상충되는 기본권 사이에 합리적인 조화를 이루고 있는 것으로 판단된다.

<헌법재판소 2004. 8. 26 - 2003헌마457- 기본권 서열이론이 채택된 판례>

흡연자들이 자유롭게 흡연할 권리를 흡연권이라고 한다면, 이러한 흡연구능은 인간의 존엄과 행복추구권을 규정한 헌법 제10조와 사생활의 자유를 규정한 헌법 제17조에 의하여 뒷받침된다. (중략) 인간으로서의 존엄과 가치를 실현하고 행복을 추구하기 위하여서는 누구나 자유로이 의사를 결정하고 그에 기하여 자율적인 생활을 형성할 수 있어야 하므로, 자유로운 흡연에의 결정 및 흡연행위를 포함하는 흡연권은 헌법 제10조에서도 그 근거를 찾을 수 있다. (중략) 흡연자들의 흡연권이 인정되듯이, 비흡연자들에게도 흡연을 하지 아니할 권리 내지 흡연으로부터 자유로울 권리가 인정된다. 흡연권은 흡연권과 마찬가지로 헌법 제17조, 헌법 제10조에서 그 헌법적 근거를 찾을 수 있다. 나아가 흡연이 흡연자는 물론 간접흡연에 노출되는 비흡연자들의 건강과 생명도 위협한다는 면에서 흡연권은 헌법이 보장하는 건강권과 생명권에 기하여서도 인정된다. 흡연자가 비흡연자에게 아무런

영향을 미치지 않는 방법으로 흡연을 하는 경우에는 기본권의 충돌이 일어나지 않는다. 그러나 흡연자와 비흡연자가 함께 생활하는 공간에서의 흡연행위는 필연적으로 흡연자의 기본권과 비흡연자의 기본권이 충돌하는 상황이 초래된다. 그런데 흡연권은 위와 같이 사생활의 자유를 실질적 핵으로 하는 것이고 혐연권은 사생활의 자유뿐만 아니라 생명권에까지 연결되는 것이므로 혐연권이 흡연권보다 상위의 기본권이라 할 수 있다. 이처럼 상하의 위계질서가 있는 기본권끼리 충돌하는 경우에는 상위기본권우선의 원칙에 따라 하위기본권이 제한될 수 있으므로, 결국 흡연권은 혐연권을 침해하지 않는 한에서 인정되어야 한다.

<대법원 1988. 10. 11.- 85다카29- 법익형량의 방법을 사용한 판례>

언론, 출판 등 표현의 자유는 가끔 개인의 명예나 사생활의 자유와 비밀 등 인격권의 영역을 침해할 경우가 있는데 표현의 자유 못지않게 이러한 사적 법익도 보호되어야 할 것이므로 인격권으로서의 개인의 명예의 보호와 표현의 자유의 보장이라는 두 법익이 충돌하였을 때 그 조정을 어떻게 할 것인지는 구체적인 경우에 사회적인 여러 가지 이익을 비교하여 표현의 자유로 얻어지는 이익, 가치와 인격권의 보호에 의하여 달성되는 가치를 형량하여 그 규제의 폭과 방법을 정해야 할 것이다.

<헌법재판소 2007. 10. 25. -2005헌바96- 종합적으로 고려된 사례>

채권자취소권이 행사되면 채권자의 재산권인 채권의 실효성은 확보될 수 있는 반면, 채무자와 수익자 간의 법률행위가 취소되고 수익자가 취득한 재산이 채무자의 회복되게 됨으로써 채무자 및 수익자의 일반적 행동의 자유 내지 여기에서 파생되는 계약의 자유와 수익자의 재산권이 제한되는 결과를 가져오게 된다. 즉 이 사건 법률조항으로 인하여 채권자의 재산권과 채무자 및 수익자의 일반적 행동의 자유, 그리고 채권자의 재산권과 수익자의 재산권이 동일한 장에서 충돌하는 문제가 발생하게 되는 것이다. 따라서 이 사건의 쟁점은 이러한 기본권의 충돌과 그

해결방법이고, 구체적으로는 채권자취소권제도의 목적의 정당성과 채권자취소권의 행사로 인하여 제한되는 채무자와 수익자의 기본권제한의 정도가 비례성을 유지하고 있는가가 문제된다. (중략) 이 사건 법률조항은 채권자에게 채권의 실효성 확보를 위한 수단으로서 채권자취소권을 인정함으로써, 채권자의 재산권과 채무자와 수익자의 일반적 행동의 자유 내지 계약의 자유 및 수익자의 재산권이 서로 충돌하게 되는바, 위와 같은 채권자와 채무자 및 수익자의 기본권들이 충돌하는 경우에 기본권의 서열이나 법익의 형량을 통하여 어느 한 쪽의 기본권을 우선시키고 다른 쪽의 기본권을 후퇴시킬 수는 없다고 할 것이다. 사적자치의 원칙은 헌법 제10조의 행복추구권 속에 함축된 일반적 행동자유권에서 파생된 것으로서 헌법 제119조 제1항의 자유시장 경제질서의 기초이자 우리 헌법상의 원리이고, 계약자유 원칙은 사적자치권의 기본원칙으로서 이러한 사적자치의 원칙이 법률행위의 영역에서 나타난 것이므로, 채권자의 재산권과 채무자 및 수익자의 일반적 행동의 자유권 중 어느 하나를 상위 기본권이라고 할 수는 없을 것이고, 채권자의 재산권과 수익자의 재산권 사이에서도 어느 쪽이 우월하다고 할 수는 없을 것이기 때문이다. 따라서 이러한 경우에는 헌법의 통일성을 유지하기 위하여 상충하는 기본권 모두가 최대한으로 그 기능과 효력을 발휘할 수 있도록 조화로운 방법을 모색하되(규범조화적 해석), 법익형량의 원리, 입법에 의한 선택적 재량 등을 종합적으로 참작하여 심사하여야 할 것이다.

3) 검토

실제로 기본권이 충돌하는 경우 그에 대한 해결은 항상 입법에 의해서만 이루어지는 것은 아니고 헌법해석을 통해서도 이루어진다. 또한 헌법적인 문제인 기본권 충돌의 문제를 전적으로 입법자의 재량에 맡겨놓는 것은 바람직하지 않을 수 있으며, 이 방법으로 충돌을 조정하는 것이 항상 타당한 방법이 되는 것은 아니기에 입법형성의 자유이론은 그것만으로는 충분하다고 볼 수 없다. 또한 모든 개별 기본권들을 서열화하는 것은 불가능하고, 서열화하는 기준이 절대적이고 객관적이라고 볼 수도 없기 때문에 기본권 의 서열이론도 문제가 있다. 그리고 법익형량이

론은 법익과 법익간의 중요성을 비교한다고는 하지만, 기본적으로 기본권의 서열을 전제로 하여 성립되는 이론이라고 할 수 있기 때문에 이것만으로도 적절한 해결방법이 된다고는 볼 수 없다. 따라서 마지막 방법으로 주어지는 규범조화적인 방법이 기본권이 충돌하고 한 개의 기본권을 도저히 포기할 수 없는 상황에 있어서는 비교적 효과적이면서도 타당한 해결방법이 될 것이다.

결론적으로 기본권의 충돌을 해결하기 위해선 우선적으로 어떠한 기본권이 가장 직접적인 관련성을 갖는 것인가를 고려해야 할 것이다. 그리고 양자택일이 어느 정도 가능하다고 할 수 있는 경우에는 우월적인 가치의 기본권을 보호하는 쪽으로 선택을 하고, 양자택일이 도저히 불가피한 경우에는 법익형량을 모두 고려해 본 상태에서 상대적으로 우월한 지위에 있는 기본권을 보호하기로 한다. 그러나 그렇게 할 수 없는 경우에는 충돌하는 기본권을 모두 실현시킬 수 있는 적절한 조화점을 찾아 이를 해결하는 것이 타당하다고 본다.

4. 소 결

지금까지 두 개 이상의 기본권이 충돌을 할 때 어떠한 점들이 문제가 될 수 있으며, 그 문제에 대한 해결방안으로는 어떤 것들이 있는지를 살펴보았다. 생각해보건대, 기업들이 소비자의 개인정보를 이용하여 온라인 맞춤형 광고를 하는 상황은 분명히 개인이 가지고 있는 ‘개인정보자기결정권’의 일정부분 제한을 가하는 것이라고 할 수 있다. 그러나 광고주체가 가지고 있는 ‘광고 표현의 자유’또한 헌법적으로 인정되는 기본권이다. 또한, 자유로운 경제활동이 헌법적으로도 장려되는 대한민국의 현실에서는 기업의 광고활동은 필수불가결한 것으로 기업의 광고가 단순히 상업적인 의도로서 뿐만이 아니라 소비자의 알권리를 충족시켜준다는 점에서 공익적인 면도 인정되고 있음을 부정할 수는 없다.

한편으로, 국민 개인에게 헌법상으로 보장되는 ‘개인정보 자기결정권’은 “자신과 관계된 정보의 흐름을 통제하는 권리”, “언제 어떠한 한계 내에서 개인적 생활을 공개할 것인지를 원칙적으로 스스로 결정하는, 개인적 자기결정의 사상에서 나오는 권리”이기 때문에 그것에 대한 보호 또한 매우 중요한 것이라고 할 수 있다.

하지만 명심할 것은 개인정보 자기결정권을 통해 보호되는 개인의 권리는 그것이 다른 법률에서 규정한 ‘개인정보’의 개념에 포함되는 범위 하에서 인정되어야 한다는 것이라는 점이다.

소비자의 행태, 성향, 위치 정보가 그 사람의 다른 식별개인정보와 쉽게 결합하여 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’에서 규정한 개인정보의 영역에 들어갈 수 있다고 할지라도 그것이 실제로 결합되지 않는 한 단순히 가능성으로 존재한다고 하여, 그것을 개인정보의 영역에 포함시켜 법이 규정하고 있는 범위의 외연을 함부로 넓히는 것은 소비자의 권리를 과도하게 강조한 나머지 현대사회에서 역시 존중되어야 할 기업의 광고표현의 자유를 억압하는 것이라고 할 수 있다. 비식별 개인정보는 그것이 다른 정보와 결합되지 않는 이상 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’에서 언급한 개인정보라고 볼 수 없다. 그러므로 비식별개인정보의 개념을 명확히 정의하면서 그 의미의 외연을 확정하는 것을 통해, 두 가지의 기본권이 충돌하는 현재의 시점에서 ‘개인정보 자기결정권’과 ‘광고표현의 자유’가 규범조화적으로 같이 공존할 수 있는 적절한 균형점 또한 찾을 수 있을 것이라고 생각한다.

제5장 개인정보자기결정권의 보호에 관한 외국입법례

제1절 OECD

개인정보의 노출과 그것에 대한 불법적인 침해로 인해 발생하는 피해는 비단 대한민국에 국한된 문제만은 아니다. 새로운 통신기술의 발달에 따라 개인정보의 보호에 대한 문제가 전 세계적으로 이슈화되면서, 각 국에서도 이에 발맞추어 개인정보 유출로 인한 피해를 최소화하기 위해 그것을 예방하는 한편, 예상되는 문제들에 대한 방향지침을 마련할 수 있도록 관련 법률과 규범들을 제정하는 움직임이 보이고 있다. 각 국의 개인정보 보호 관련 입법례들을 살펴보기 전에 여러 국가에 걸쳐 적용되고 있는 국제기구 OECD의 규범을 먼저 살펴보고, 그러한 내용들이 각국의 특성에 따라 어떻게 변형되어 적용되고 있는지 알아보자.

국제기구인 OECD에서는 1980년도에 개인정보에 관한 가이드라인³²⁾(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)을 만들어 세계 각국의 프라이버시 문제와 관련하여 일반적인 원리를 확립하였다. 이는 비록 회원국의 활동을 직접적으로 제한하는 구속력은 없지만, 30여년이 지난 지금에도 여러 국가의 개인정보 보호 법률에 영향을 미치며 개인정보의 수집과 가공에 관한 문제에 대한 기본적 지침이 되고 있다. 이 가이드라인을 통해 OECD는 ‘개인정보’에 대해 개인을 식별하거나 식별가능하게 하는데 관련이 있는 어떠한 형태의 정보(any information relating to an identified or identifiable individual)라고 정의를 내렸다.

OECD 가이드라인은 크게 5가지로 구성되어 있다. 개인정보에 대한 정의를 포함하고 있는 General Definitions 부분으로부터 시작하여, 두 번째 파트는 한 국가 안에서 적용되는 기본 원칙(Basic Principles of national application)을 담고 있다. 세 번째 파트는 개인정보의 흐름과 합법적인 제한에 대한 내용과 함께 국제적 적용에 기본 원칙에 대한 규정(Basic Principles of international applications: Free

32) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Flow and Legitimate Restrictions)이고, 네 번째, 다섯 번째 파트는 각각 국내적 실행(National Implementation)과 국제적 협력(International Co-operation)에 관한 내용을 담고 있다.

각 부분의 내용을 표로 정리해보면 다음과 같다.

Part	Topic	Contents
1	General Definitions	- 정보와 관련된 용어들에 대한 정의 - 지침의 범위
2	Basic Principles of national application	- 정보 수집의 제한 - 정보의 질에 관한 원칙 - 정보 수집의 목적에 관한 원칙 - 수집된 정보의 사용과 제한에 관한 원칙 - 보안의 원칙 - 공개의 원칙 - 개인 참여에 관한 원칙 - 책임의 원칙
3	Basic Principles of international applications: Free Flow and Legitimate Restrictions	- 다른 국가의 정보 처리에 대한 고려원칙 - 정보 교류에 관한 제한과 원칙 - 자유 교환에 방해되는 법, 제도 금지의 원칙
4	National Implementation	- 적절한 국내법을 적용할 것 - 자기 규제에 관한 격려와 지원 - 법 적용에 실패할 경우에 대비한 보완책 마련 - 정보사용과 관련하여 불평등한 차별 방지
5	International Cooperation	- 다른 국가에 자국법규 확인시키기 - 정보 교환을 위한 격려와 상호 협력 - 정보 이동을 위한 원칙 마련

[표 5-1]

이어서 OECD는 2002년에 이르러 정보보안 및 프라이버시 작업팀(Working Party for Information Security and Privacy)의 주도하에 1980년 가이드라인의 개정작업을 추진하여, ‘정보시스템과 네트워크보안을 위한 OECD 가이드라인(OECD Guidelines for the Security of Information Systems and Network)’이라는 이름으로 ‘1) 인식 2) 책임 3) 대응 4) 윤리 5) 민주주의 6) 위험평가 7) 보안설계와 이행 8) 보안관리 9) 재평가’ 등 9가지의 보안원칙에 대한 내용을 담은 새로운 가이드라인을 공식 발표하였다.

이를 바탕으로 2006년에 발행된 OECD report³³⁾에 따르면 OECD가 새로 마련한 ‘개인정보 보호정책의 고지(Privacy Notice)’는 새로 개정된 OECD Guidelines의 실행을 돕기 위한 유용한 도구로서, 그러한 고지는 짧고 간단해야하며 정보를 사용하는 개인들로 하여금 정보를 자기화함으로써 유용하게 사용할 수 있도록 하는데 도움이 되어야 한다고 역설하였다. OECD가 그들의 개인정보에 대한 기존 연구들과 현행 안에 기초하여 효율적인 개인정보 보호를 위해 각 회원국의 조직들에 권고한 핵심사항들은 이와 같다.

1. Identify data flows: 개인정보의 수집, 사용, 공유, 보호, 폐기와 관련하여 조직의 관행들을 파악하고 있어야 한다.
2. Conduct a legal review: 어떠한 법, 규제, 산업관련 법령, 계약, 협약 또는 다른 법적 요건들이 당신의 조직의 개인정보 수집과 사용에 대해 관장하고 있는지 알고 있어야 한다.
3. Prepare a comprehensive privacy policy statement: 당신의 조직의 개인정보 보호 정책과 실행에 대해 많은 사람들이 포괄적으로 이해할 수 있도록 문서를 작성해야 한다. 그리고 이 문서의 정확성을 확보하기 위해 내부적으로 많은 검토를 해야 한다.

33) OECD (2006), “Making Privacy Notices Simple: An OECD Report and Recommendations”, OECD Digital Economy Papers, No. 120, OECD Publishing.

4. Develop a simplified notice: 소비자들이 그들의 개인정보가 어떻게 사용되고 있는지 쉽게 이해할 수 있도록 중요 정보를 포함한 짧고 명확한 고지방법을 개발해야 한다.
5. Test the usability of the notice: 간결화된 고지방법이 사용자에게 이해가 쉽고 그들에게 친화적인지를 알기 위해 테스트를 해야한다.
6. Disclose the simplified notice: 간결화된 고지를 조직의 웹사이트에 공개하거나 소비자에게 분배하여 개인의 정보가 사용될 소비자가 그것을 쉽게 접근하고 읽을 수 있도록 해야 한다. 포괄적으로 세부사항에 대해서도 알고자 하는 사람들을 위해 보다 쉬운 접근을 보장해야 한다.

[표 5-2]

세계 선진국들의 모임인 OECD에서는 이처럼 오래전부터 개인정보 보호의 필요성에 대해 절감하고 있었고, 1980년대부터 현대에 이르기까지 지속적으로 개인정보 보호에 대한 규범들을 마련하여 관련 문제에 대한 지침을 세웠다. OECD의 회원국들이 비록 독자적으로 법률과 행동지침들을 마련한다고 하더라도 국가 간 개인정보보호의 수준이 현저하게 다를 수 있기 때문에, OECD의 가이드라인과 개인정보보호의 고지는 국제기구 차원에서의 통합적인 지침으로서의 의미를 지닌다고 말할 수 있다. 이로 인해 회원국들은 자국 내에서 개인정보 보호에 대한 움직임을 보다 가속화할 수 있고, 궁극적으로 국가 상호간에 정보보호 수준이 균형이 맞춰짐으로써 개인정보 보호 수준이 다르면서 발생할 수 있는 국제 상거래에서의 장애요인들을 줄이는 데에도 긍정적인 영향을 미치고 있다. 여러 국가들은 이러한 기준에 맞추어 각국의 정보보호 관련 법규를 마련하고 있는데, OECD 국가들 중 미국과 유럽연합에 대해 살펴보고 그들은 이러한 개인정보 문제에 대해 어떻게 접근하며 어떠한 법규들을 제정하였는지, 그리고 비식별 개인정보 문제에 대해선

어떻게 대처하고 있는지 알아보기로 하자.

제2절 미국

1. 미국 개인정보보호 관련 법률의 체계

미국에서 프라이버시의 보호와 관련하여 입법화 논의가 진행된 것은 1972년에 있었던 ‘워터게이트 사건’으로부터 시작된다. 이로 인해 1974년에 현대적으로는 최초로 프라이버시의 권리가 포함된 ‘Privacy Act of 1974’가 입법화되었다. 미국의 개인정보보호 법률은 공공부문과 민간부문이 분리되어 각 분야에서 필요에 의해 개인정보보호법규를 정비하는 ‘개별법 체계’를 따르고 있으며 공공, 민간부문을 모두 통합적으로 포괄하는 개인정보 보호 법률이 정비되어 있지는 않은데, ‘Privacy Act of 1974’는 미국 공공영역 부문에 한정되어 일반법적인 역할을 담당하고 있다. 한편 민간 부문에선 통신, 의료, 가족 교육, 비디오 프라이버시, 건강보험, 전화, 운전자, 컴퓨터 사기 등 다양한 영역에서 개별 분야별로 프라이버시 보호를 목적으로 한 법률이 제정되고 있다. 이처럼 미국의 ‘개별법 체계’는 사회 각 분야에서 개인정보 보호에 대한 필요성이 제기될 때 그 요구에 맞는 법규가 제정됨으로써 사회적인 요구에 융통성 있게 대응할 수 있다는 장점이 있으나, 그 입법과 관련된 이익단체들의 영향을 쉽게 받을 수 있다는 점에서 단점도 존재한다고 볼 수 있다. 미국의 개인정보보호 법률 체계를 표로 정리하면 다음과 같다.

	공공부문	민간부문
일반법	Privacy Act of 1974	-
개별법	Freedom of Information Act(1966) E-Government Act of 2002 Security Breach Notification Law -California Senate Bill	Fair Credit Reporting Act(1970) Family Educational Rights and Privacy Act of 1974 Fair Debt Collections Practices Act(1978) Right to Financial Privacy Act of

	1386(2003)	1978 Privacy Protection Act of 1980 Cable Communications Policy Act of 1984 Video Privacy Protection Act of 1988 Health Insurance Portability and Accountability Act of 1996 Federal Information Security Management Act of 2002 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 Junk Fax Prevention Act of 2005 Telephone Records and Privacy Protection Act of 2006
--	------------	--

[표 5-3]

Privacy act of 1974를 살펴보면 ‘개인식별정보’(personally identifiable information)와 같은 단어 자체는 사용되지 않고 있으나, 기록(record), 기록의 체계(system of records), 통계적 기록(statistical record)에 대한 정의가 나와 있다. 그 중 Record에 대한 정의를 살펴보면 ‘교육수준, 금융거래기록, 범죄기록, 의료기록, 고용기록 등에 한정되지 않지만 한 개인의 이름과 주민 번호, 지문, 목소리, 사진과 같은 개인을 특별히 특정할 수 있는 상징 등을 포함하고 있는 정보 혹은 그것의 모음’이라고 할 수 있다. 이것을 보면 역시 한국의 법규와 마찬가지로 일반적인 기준에서 개인식별정보 혹은 식별가능한 개인정보에 대하여 범위를 잡고 있는 듯하다.

한편으로 온라인 기술의 발달과 정보 개념의 확대와 더불어 민간 부문에서는 꾸준히 관련 법규들이 제정되고 있다. 또한 개인정보의 침해 문제가 빈번해지자 관련 법규의 제정과 더불어 기존 법규로 인한 처벌이 강화되고 있으며 조금씩 그

적용범위의 확대도 이루어지고 있다. 전화통신 프라이버시 보호 및 불법 기록방지에 대한 법률(Telephone Records and Privacy Protection Act of 2006), 유전자 정보에 대한 보호 및 차별 금지에 대한 법률(Genetic Information Nondiscrimination Act of 2008) 등 새로운 법규의 제정을 통해 개인정보의 보호범위를 점차 넓혀가는 노력을 기울이고 있으며, PII를 사용, 수집하는 모든 기관들이 수집한 국민 개인의 정보를 노출하거나 정보 소유자의 정보 보호 의무를 위반했을 경우에 그 사실을 고지하도록 하는 Data Breach Notification Act가 제안되었고, 보안 위반 사건에 대한 전국적으로 고지를 함으로써 소비자를 보호하는 것을 목적으로 하는 Data Accountability and Trust Act는 현재 하원을 통과한 상태이다. 또한 미국에서는 지속적인 ID 도용범죄로 인한 피해를 예방하고 그것에 대한 처벌규정을 강화하는 움직임을 추진하고 있고, 데이터 침해 시 고지 뿐만이 아니라 다른 면으로 합리적인 보안정책 및 절차를 준비하고자 한다. 최근 미국에서 제안된 법률안들을 정리하면 다음과 같다.

	법률(안) 목록
제·개정 법률 및 제안법안	Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003
	Genetic Information Non-discrimination Act of 2008
	Family Educational Rights and Privacy: Final Rule
	Data Breach Notification Act
	Free Flow of Information Act of 2009
	Student Privacy Protection Act of 2009
	Data Accountability and Trust Act

[표 5-4]

여기서 주목할 점은 미국에서도 역시 아직 소비자의 행태정보와 위치정보 등 비식별 개인정보와 관련되어선 그것을 확실하게 규율할 수 있는 법규가 제대로 정비되지 않았다는 점이다. 사생활 보호를 위해서 위치정보법도 발의된 바 있지만,³⁴⁾ Opt-In v. Opt-out 방식의 논란 속에 헌법상의 기본권인 자유를 침해한다는 이유로 법률이 통과되지 못하고 있다.

확정된 법규는 아니지만, 미국 FTC(Federal Trade Commission)에서는 이와 관련하여 행태정보 기반의 온라인 광고로 인해 발생할 수 있는 프라이버시 침해 문제에 대처하기 위해 산업계, 학계, 이용자 등의 의견을 수렴하여 2009년 2월경에 “온라인 행태 광고에 대한 자율규제 원칙(Self-Regulatory Principles for Online Behavioral Advertising)”을 발표하였다.³⁵⁾ FTC에서 만든 가이드라인에 따르면 그 기본원칙으로서 제시되는 것들은 다음과 같다.

- 1) 투명성 및 소비자 통제권(Transparency and Consumer Control)
- 2) 소비자 정보에 대한 합리적인 보안과 정보 보유제한(Reasonable Security and Limited Data Retention for Consumer Data)
- 3) 기존 프라이버시 정책에 대한 중대한 변경 시 명시적 동의 획득(Affirmative Express consent for Material Changes to Existing Privacy Promises)
- 4) 행동 광고 목적을 위한 민감정보 이용 시 명시적 동의 획득 또는 금지(Affirmative Express Consent to(or Prohibition Against) Using Sensitive Data for Behavioral Advertising)

이 보고서에 대해 사람들이 FTC에게 가장 궁금하다고 요청한 공통적인 관심사는, 이 가이드라인이 개인정보와 관련하여 어느 정도의 범위까지 보호대상으로 놓는 지에 관한 내용이었다. 예를 들어 이 가이드라인에 대하여 논평하는 사람들은 개인정보 중에서 식별가능하지 않은 정보(data that is not personally identifiable)가 이 가이드라인을 통해서 보호될 수 있는 부분에 속하는지에 대하여 심각하게 논의하였다, 그에 대하여 FTC는 이 가이드라인이 사생활 침해와 관련된 소비자

34) 예컨대, 위치프라이버시보호법('01), 무선프라이버시보호법('01, '03, '05)이 발의된 바 있음.

35) <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf> (2010.8.25. 방문).

개인정보 보호에 있어선 특정한 소비자, 컴퓨터 그리고 다른 기타 개인을 식별할 수 있는 장치들과 연관될 수 있는 것이라고 하면 어떤 정보라도 그 보호의 대상이 되어야 한다고 대답하였다. 그리고 소비자와 관련하여 개인적으로 민감한 정보의 수집 및 이용 등에 의하여 제기되는 사생활 침해 이슈가 점차 불거짐에 따라, 이 가이드라인은 회사들로 하여금 온라인 맞춤형 광고를 제공하기 위한 개인정보를 수집하기 전에 꼭 소비자들로부터 명시적인 동의를 받게끔 하도록 촉구하였다.

한편으로는 이 가이드라인이 너무 보호의 폭을 줄인 것이 아니냐는 비판도 제기되었다. 온라인과 오프라인을 막론하고 소비자 프라이버시 침해에 대한 위협은 상존하고 있으며, 온라인 맞춤형 광고는 그 많은 문제 중에서 단 한 개의 예를 대표하는 것일 뿐이니, 보다 다방면에 있어 소비자 프라이버시를 보호할 수 있는 보다 넓은 영역의 법이 만들어져야 한다고 그들은 주장하였다. 실제로 이 가이드라인은 기업들에게 규제 지침을 알려주고 방향성을 제시해주었다는 점에서는 큰 의의를 둘 만 하지만, 기업들을 확실히 압박할 수 있는 강한 규제보다는 스스로 자율적으로 규제할 수 있는 여지를 아직은 열어주고 있다는 점에서 상대적으로 느슨한 면이 있다는 비판도 받기도 한다. 비식별 개인정보의 보호와 규제에 관해선 미국에서도 아직 논쟁의 여지가 존재하는 가운데, 이러한 움직임과 더불어 확대되는 소비자 개인정보 관련 침해 이슈에 대응할 수 있도록 하기 위하여 현행 법률의 적용범위를 확대하고 그것의 처벌규정을 강화하는 방식으로 대응하고 있다.

미국의 경우에는 민간의 자율규제가 중시되고 있는데, 위치정보의 경우에도 CTIA(Cellular Telephone Industries Association)에서 LBS 이용에 관한 지침을 마련하여 사업자들이 자율적으로 위치정보를 보호하고 있다. CTIA의 가이드라인은 적법성과 공정성에 기초하는 고지(Notice), 동의(Consent), 보안과 보존(Security & Integrity), 그리고 기술 중립성을 포함하고 있다.³⁶⁾

36) Best Practices and Guidelines for Location Based Services:

http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (2010.8.24. 방문).

2. 개인정보의 침해와 관련 사례들 살펴보기

가. Remsburg v. DocuSearch 사건

1999년 미국 New Hampshire에선 인터넷 정보 사이트(SNS)를 이용해 자신이 따라다니던 젊은 여성의 사회보장번호와 직장주소를 알아낸 스토키가 결국 그 여성의 직장을 찾아가 그녀에게 충격을 가하는 사건이 발생했다. 이 사건은 물론 현재 논란이 되고 있는 동적개념으로서의 위치정보의 문제는 아니라고 할 수 있지만, 정적인 정보라 할지라도 개인을 특정할 수 있는 위치정보가 범죄에 있어 악용될 경우에 예상할 수 없는 악영향을 초래할 수 있다는 점에서 사회에 경각심을 심어 주는 사례이다. 이 사건에 대해 2003년 2월 New Hampshire 대법원은 개인정보를 제대로 관리하지 못하고 무분별하게 다른 이에게 판매함으로써 유발된 문제에 대해선 그 정보를 제대로 관리하지 못한 정보의 중개인, 중개상들에게 책임이 있을 수 있다고 판시하였다.³⁷⁾

나. Choice Point 사 사건³⁸⁾

미국에서는 데이터 브로커라고 하여 개인정보를 수집하고, 그것을 가공하여 다른 곳에 판매하는 새로운 산업 형태가 등장하게 되었다. 2000년대 중반에는 이러한 회사들이 미국 내에서 150개 이상으로 증가하였는데 결국 이들을 통해 50만 명이 넘는 미국 국민의 개인정보가 불법으로 노출되는 사건이 일어나게 되었다. 이 중 가장 크게 이슈가 된 사건은 미국의 개인정보 관리업체 중의 하나인 'Choice Point' 사의 사건이다. 불과 5년여 전의 일이지만, 그 당시만 해도 미국 국민들은 그들의 개인 정보의 불법 유출에 대하여 별다른 신경을 쓰지 않고 있었다. 이러한 정보 보호의 필요성에 대한 공감대가 낮아서였는지, 신분 도용자들은 합법적인 사업자로 위장하여 Choice Point 사의 데이터베이스에 접근하였고, 이로 인

37) Remsburg v. Docusearch, 816 A.2d 1001, 149 N.H. 148 (N. H. 2003).

38) 한국정보보호진흥원, 인터넷 개인정보 노출방지 및 프라이버시 보호 방안 연구, 2007. 12, pp.59-62.

해 캘리포니아 주민 3만 5천여 명의 정보가 유출되게 되었으며, 그 여파가 미국 전역으로 퍼져 2004년 말경에는 피해자가 통합 14만 명을 상회하는 것으로 조사되었다. 실제로 신분 도용자들은 2003년부터 이전에 훔친 타인의 개인 신용정보를 사용하여 사업허가증을 위조로 발행하여 사업허가서와 신청서를 Choice Point에 보내 정보 접근 권한을 획득하였고, 그러한 방법으로 얻은 접근 코드와 비밀번호를 가지고 회사 데이터베이스의 1만 7천여번이나 접근을 하여 다른 이들의 정보를 빼내었다.

이 사건에 대해 미국 연방거래위원회(FTC)에서는 2006년 1월, 개인정보 취급에 대한 소비자 권리침해 등을 이유로 1천만 달러 벌금 및 5백만 달러의 손해배상을 결정하였다. 이는 미 FTC가 부과한 벌금과 손해배상액 사상 그 당시의 최고가액이었으며, 손해배상이외에도 벌금을 물리는 등 ‘징벌적 배상제도(Punitive Damages)’를 도입함으로써 향후 개인정보 유출에 대해 엄금을 하겠다는 미국 정부의 태도를 보여주는 사례라고 부를 수 있겠다.

Choice Point 사 사건이 시사하는 바는 현대 사회에서는 인터넷 기술과 통신 기술의 발달로 인하여 자기 자신도 모르는 사이에 개인의 정보가 타인에 의해 불법적으로 획득되어 악용될 수 있다는 것과, 데이터 브로커에 대한 미국 연방정부 차원에서의 대응 및 법률 규제가 꼭 필요하다는 것이다. 그러한 결과 몇몇 주에서 선도적인 움직임을 보여 2006년 9월경에는 33개의 주가 개인정보 불법접근에 대해 소비자에게 직접 통보를 하는 법안을 통과시키게 되었다. Choice Point 사건이 발생했을 당시에 이러한 법안이 시행되고 있었던 주는 오로지 캘리포니아 주 뿐이었지만, 이 일을 계기로 많은 변화가 있게 된 것이며, 뉴욕 주에서는 통보 의무가 다른 주들에 비해 더욱더 강화되기도 하였다.

다. 소비자의 행태정보를 광고주에게 판매하는 마켓플레이스³⁹⁾

데이터 브로커는 이제 정태적인 정보 판매와 중개에서 벗어나 여행, 자동차, 소매 쇼핑 등과 관련하여 인터넷상으로 수집한 미국 소비자들의 이용자 행태 데이

39) 한국인터넷진흥원, 인터넷 이슈분석 및 기초정책자료 발굴 위탁용역, 2009. 12, pp. 132-134.

터들을 데이터베이스화하여, 소비자에게 맞춤형 광고를 제작하려는 광고주에게 판매하는 등 그들의 사업의 대상을 동태적 정보에 있어서까지 확장하고 있다. 대표적인 사업자는 Blue Kai와 eXelate Media이다.

이러한 회사들이 소비자의 행태정보를 중개함으로써, 광고기업들은 이용자들의 행태를 유형별로 분류하고 각 소비자들의 성향을 파악하여 소비자가 맘에 들어할 만한 상품을 미루어 짐작하여 그 소비자에게 맞춤형 광고를 보내게 된다. 예를 들어 서울에 있는 사람이 도쿄행 비행기표를 예매했다면 도쿄에 위치한 관광지와 호텔 광고가 비행기표 예매자에게 자주 노출되는 형식이라고 할 수 있다.

소비자의 행태 수집 및 분석은 현행 법 상으로 개인 정보의 침해와 관련하여 굉장히 민감한 문제이기 때문에 개인의 프라이버시를 옹호하는 미국의 NGO들은 미국의 에너지, 통상 하원 의원회 내의 통신기술 인터넷 소위원회(the House Energy and Commerce Subcommittee on Communications, Technology and the Internet)에 이와 관련한 법률을 제정하자는 요청을 지속적으로 하고 있고, 민주당 의원인 릭 바우처(Rick Boucher)는 어떠한 정보가 수집되며 그 정보가 어떠한 방향으로 사용되는지에 대해 규제할 수 있는 법안을 소비자 보호 소위원회 의장인 바비 러쉬(Bobby Rush)와 인터넷 소위원회 소속 공화당 의원 클리프 스테른(Cliff Stearn)과 함께 준비하고 있다. 바우처 의원의 의견에 따르면 이 법률안은 온라인 사업을 방해하려고 하는 것이 아니고, 인터넷 이용자들이 전자상거래와 온라인 서비스에 대해 더욱 신뢰할 수 있도록 하기 위한 것이다. 법안의 입법 목적은 인터넷 이용자가 본인의 어떤 정보가 이용되고 수집되는지를 스스로 알기 위함이며, 인터넷 업체들로 하여금 ‘소비자 맞춤형 광고’ 제작을 위해 이용자들의 웹 서핑 내역을 추진할 때 반드시 이용자의 승인을 받도록 규정하고 하기 위함이다.⁴⁰⁾ 보다 세부적으로 들어가면 정보 수집 방식에 있어선 소비자 단체에서 주장하는 방식인 Opt-in방식(정보 수집 이전에 이용자 동의를 구하도록 하는 사전 승인 방식)과 온라인 사업자들이 주장하는 Opt-out 방식(일단 사업자들은 소비자의 정보를 자유로이 수집하며 정보 수집을 원하지 않는 소비자가 사후적으로 그것을 거부하는 방식)과의 대립이 있는 상태이고, 정보들이 자동적으로 수집된다고 할지라도

40) http://www.redorbit.com/news/technology/1748844/house_bill_takes_aim_at_web_privacy/ 참조.

의료, 금융, 사회보장번호와 같은 개인에 있어서 민감한 정보들은 무조건 사전 동의 식으로 가야한다는 의견에는 전반적인 동의가 일고 있다. 실제로 미국 펜실베이니아, 버클리 대학에서 조사한 바에 따르면 미국 인터넷 이용자의 약 2/3은 소비자 맞춤형 광고를 위한 온라인 행동 추적에 반대하는 것으로 나타나고 있어, 이와 관련하여 미국 의회의 관련 법 제정이 어떤 방식으로 이루어질 것인가 귀추가 주목이 되고 있다.⁴¹⁾

라. 더블클릭(DoubleClick) 사건⁴²⁾

1) 사건의 개요

더블클릭사(DoubleClick)는 World Wide Web에서 인터넷 최대의 광고주로 사업을 전개하고 있다. “더블클릭 네트워크”라 알려진 더블클릭사는 알타비스타(AltaVista) 등 유명한 웹사이트에서 광고서비스를 제공했다. 또한 더블클릭사는 캘리포니아에 위치하여 서버를 두고 있는 11,500개의 인터넷 웹사이트에 인터넷 이용자의 컴퓨터와 웹브라우저를 추적하는 기술을 가지고 인터넷 광고 서비스를 제공하는 회사였다.

인터넷 광고대행사인 더블클릭사는 인터넷 이용자들이 자신의 고객의 광고를 보게 될 때 쿠키정보에 고유한 식별번호인 Global User ID(GUID)를 부여한 후 이용자의 컴퓨터에 쿠키정보로 저장되게 함으로써 개별 이용자들의 인터넷 이용 상황을 모니터링하여 이용자들이 인터넷 서핑을 하는 동안에 같은 내용의 광고가 반복적으로 나타나지 않도록 하였다.

더블클릭사는 이와 같이 쿠키를 통하여 개인의 인터넷 이용정보를 수집한다는 사실을 자신의 고객 사이트 등을 통하여 이용자들에게 고지하거나 동의를 받은 바는 없었으나 이러한 인터넷 이용정보를 구체적인 개인식별정보와 연결시키지 않았으므로 처음에는 이와 같은 관행이 문제가 되지는 않았다.⁴³⁾

41) <http://www.reuters.com/article/idUSN0610413720091007>

42) 김범수 외, 디지털 프라이버시와 법률, 한국학술정보, 2009, 98-106면 참조.

43) Courtenay Youngblood, A New Millennium Dilemma: Cookie Technology, Consumers, And the Future of the Internet, 11 J. Art & Ent. Law, 45, 52.

그러나 더블클릭사는 여기에서 그치지 않고 1999. 11. 카탈로그 마케팅을 하는 미국 내 1,100여 개 디렉트마케팅 업체로부터 개인들의 물품 구매정보 및 홈쇼핑 습관 등에 관한 정보를 수집하여 카탈로그 마케팅에 관한 한 가장 큰 데이터베이스를 보유한 회사인 아바커스(Abacus)사를 합병함으로써 사회적 문제가 되기 시작하였다.

이 과정을 보다 상세히 살펴보면 다음과 같다. 즉 어떤 인터넷 이용자가 웹사이트에 가입하기 위해 방문했을 때 '쿠키(cookie)'는 이용자들의 컴퓨터에 장착된다. 그 뒤에 그 이용자가 등록하였거나 상품을 구매하였던 웹사이트를 다시 방문했을 때 이용자의 신원은 '쿠키(cookie)'에 연결된다. 더블클릭사는 아바커스 데이터베이스의 이용을 통해 이용자에 대한 막대한 양의 개인정보를 얻을 수 있다. 인터넷 이용자의 구매습관, 광고에 대한 반응과 이용자가 웹사이트를 방문하는 것은 쿠키를 통해 계속적으로 추적되고 기록된다. 인터넷 사용자는 인터넷을 빈번하게 이용하고 그들의 개인적인 흥미를 추구할 뿐 아니라 개인의 특징과 서비스의 판매 목적을 위해 자주 이용한다.

예컨대, 성인용 인터넷 웹사이트를 방문하여 성인용 제품을 구매할 수도 있다. 또한 법률 관련 사이트, 정치, 행정 관련 사이트, 도서 사이트, 비디오테이프 DVD 사이트, 그리고 온라인 बैं킹과 중개사이트를 포함한 여러 '민감한(sensitive)' 웹사이트를 방문할 수 있다. 이때 더블클릭사가 웹사이트에 가입한 인터넷 이용자에 관하여 얻을 수 있는 정보의 범위는 인터넷 이용자의 이름, 주소, 전화번호, 구매 경향과 이력, 인터넷 이용자가 방문하였던 웹사이트의 경력, 신용카드 번호와 정보, 은행예금정보, 그리고 개인 취향 등이다. 결국 더블클릭사는 방문했던 고객이나 웹사이트에 가입하였거나, 혹은 더블클릭사가 제공하였던 인터넷 배너 광고에 클릭하였던 인터넷 이용자에 대한 개인정보를 수집, 축적할 수 있게 되었다. 또한 이러한 정보는 다른 사업들과 제3자에게 제공, 유출되어 왔다. 인터넷 이용자로서는 자신의 개인 신상정보가 쿠키(cookie)에 '연결된(linked up)' 버튼이나 웹사이트의 배너 광고를 무심코 클릭함으로써 공개 내지 유출되는 위험을 감수해야 한다. 이것은 프라이버시에 대한 심각한 침해가 되었다.

2) 문제점

더블클릭 사건에 관련된 구체적인 문제점은 다음과 같다.

가) 인터넷 이용자의 개인 신상정보를 수집하는 관행이 시작된 이래로 더블클릭사는 개인적이고 비밀스러운 신상정보를 획득, 이용, 저장, 유출하고 있다는 점에 관한 정확한 사실을 정보 주체에게 정당하게 알리지 못하였다. 또한 인터넷 이용자의 개인정보자기결정권을 보장하기 위한 합법적 수단을 제공하지 못하였다. 물론 인터넷 이용자가 더블클릭사의 개인정보의 획득, 이용, 저장과 유출을 회피할 수 있는 것이 불가능하지는 않지만, 그 수단은 대부분의 인터넷 이용자의 기술적인 지식, 능력을 훨씬 넘는 전문적인 영역이다. 결국 개인정보의 획득이 회원들의 명확한 동의와 허가 없이 이루어지게 된 셈이다. 이러한 사업 관행은 캘리포니아법령, 캘리포니아 보통법상의 프라이버시권, 미연방헌법의 규정 하에서 보장되는 프라이버시권을 침해하는 불법행위로 평가된다.

나) 더블클릭사는 인터넷 사용자에게 관한 개인적인 신상정보가 수집되고 이용되지 않는다고 일반 대중에게 공표하였는데 이는 허위광고에 해당된다. 즉, 이러한 광고는 인터넷 이용자에 대한 개인정보를 수집하지 않는다고 일반인을 속인(deceive) 것이다. 비록 더블클릭사가 회원들이 이의를 제기하는 경우 개인정보의 이용을 중지하였다 하더라도 이는 이른바 옵트 아웃(opt-out)의 방법에 의해 동의를 추정하는 것으로서 허용될 수 없다.

3) 소송의 제기

2000. 1. 26. 미국의 일간지인 USA Today는 최대 규모의 인터넷 광고 대행사인 더블클릭사가 Abacus사의 데이터베이스와 쿠키를 통해 수집한 인터넷 이용자들의 인터넷 이용 정보를 결합하여, 인터넷 이용정보에 구체적인 이용자의 이름을 연결하기 시작하였다고 보도하였다. 이와 같은 보도가 있는 바로 다음 날 Harriet

Judnick이라는 여성이 캘리포니아 주 마린카운티 지방법원 (California Superior Court of Marin County)에 더블클릭사를 상대로, 더블클릭사가 쿠키를 이용하여 인터넷 이용자의 신원을 확인하고 그들의 인터넷 이용 상황을 추적하고, 이용자의 동의 없이 개인정보를 취득하였다고 주장하며, 이용자의 사전 동의 없는 쿠키 사용의 중단과 동의 없이 수집한 인터넷 이용자들의 개인정보의 파기를 구하는 소송을 제기하였다. 그동안 아무런 문제의식 없이 사용되는 쿠키의 이용에 대한 사회적인 관심을 촉발하는 계기가 마련된 것이다. 이처럼 캘리포니아의 한 여성에 의하여 시작된 더블클릭사의 쿠키정보와 오프라인 데이터베이스를 연결하려는 시도에 대한 문제제기는 여기에서 그치지 않았고, 여러 주 및 연방법원에 더블클릭사의 위와 같은 행위가 사생활 침해, 공정거래법위반, 소비자보호에 관한 법률 위반 심지어는 무단침입(trespass to property) 등에 해당한다고 주장하는 소송이 제기되었다. 연방법원에 제기된 12개의 소송 가운데 10개는 뉴욕 남부 지방법원에 제기되었다. 또한 2000. 2. 에는 연방거래위원회와 뉴욕 주 법무부장관이 더블클릭사의 업무의 정당성과 관한 비공식적인 조사를 시작하였으며, 미시건주 법무장관은 더블클릭사의 행위가 일종의 사이버 도청(cyber wiretapping)에 해당한다고 주장하며 더블클릭사를 제소하였다. 워싱턴에 본부를 두고 있는 대표적인 인터넷 프라이버시 관련 단체인 Electronic Privacy Information Center(EPIC)도 2000. 2. 10. 더블클릭사가 인터넷 이용자들의 동의 없이 인터넷 이용을 추적하고 그 정보를 마케팅 데이터베이스에 포함된 상세한 식별개인정보와 연결함으로써 불공정하고 기만적인 거래를 하였다고 주장하며 연방거래위원회에 제소하였다.

4) 당사자의 주장

가) EPIC의 주장

- (1) 쿠키나 인터넷 이용자 PC 고유의 파일을 아바커스 데이터 베이스와 합치려는 더블클릭사의 계획과 실행은 부당하다.
- (2) 개인정보의 익명성은 보장되어야 한다.

- (3) 소비자 개인신상정보를 수집함에 있어서 소비자의 동의가 필요하다.
- (4) 사이버 공간에서의 웹 서핑 감시는 오프라인에서 어떤 가게에 들르고 무엇을 구매하는지 추적하는 것과 다를 바 없다.
- (5) 실명 연계가 되면 청바지를 고르거나 알츠하이머병 또는 섹스기구에 대한 정보를 얻으려고 언제 웹을 검색했는지 속속들이 밝혀지고 이 정보가 기업이나 보험회사에 넘어가 온라인상의 빅 브라더(Big Brother)를 탄생시킬 것이다.
- (6) 더블클릭사는 고객이 다른 기업이 운영하는 웹사이트로 이동할 때에도 온라인 추적을 하였으며 몇몇 기업은 더블클릭의 추적사실도 모르고 있다.
- (7) 웹을 감시의 수단으로 변질시켜 전자상거래를 해쳐서는 안 된다.
- (8) 더블클릭사는 이용자 정보를 익명으로 수집하던 이전의 방법으로 돌아가야 한다. 실명이 아닌 익명으로도 온라인에서 충분한 광고효과를 누릴 수 있기 때문이다.
- (9) 더블클릭사는 소비자와의 개인정보보호에 대한 약속을 어겨가며 불공정하고 사기적인 수법으로 개인정보를 활용하려는 경우로서 더블클릭사와 제휴하는 다른 기업들에게 FTC가 책임을 물어야 한다.

나) 더블클릭의 주장

- (1) 인터넷은 소비자 정보를 수집하는 방식에 있어서 최대한의 이익을 추구하는 방향으로 쓰여야 한다.
- (2) 웹사이트의 대부분이 적자인 상태에서 광고회사가 소비자의 선호도를 파악하지 못하게 막는 것은 인터넷의 자유로운 사용을 위협하는 행위이다.
- (3) 웹서버의 신상정보의 수집을 밀고 나가기 전에 정부 및 업계의 가이드라인이 나올 때까지 전략상 후퇴하겠다.
- (4) 아바커스에 기록된 사람들이 현실 공간과 사이버 공간에서 보여주는 구매습관과 그들의 실제 이름 및 주소를 연결시키는 프로그램을 만드는 계획은 아직 시행되지 않은 상태이며, 소비자들에게 개인정보 수집사실을

알리고 소비자에게 선택권을 부여한 웹사이트에서만 제한적으로 사용할 것이다.

- (5) 실명 개인의 정보를 포함시킨 파일을 만들기 전에 이용자에게 ‘명확한 통보와 선택’의 기회를 제공할 것이다.
- (6) 소비자들의 입장에서 그들의 관심사항에 더 가까운 광고를 손쉽게 볼 수 있어 오히려 이득이 될 것이다.
- (7) 소비자들은 정확한 결정을 하기 위하여 필요로 하는 모든 정보를 얻게 되며 소비자에게 제때에 알맞은 메시지를 전달하여 소비자로 하여금 구매선택의 실수를 덜게 해 줄 것이다.

5) 법원의 판단

가) 캘리포니아 : 더블클릭은 인터넷 사용자의 동의를 얻지 않은 경우 인터넷 상에서의 개인정보의 취득·이용을 목적으로 쿠키를 포함한 유사기술을 사용할 수 없다. 또한 인터넷 이용자의 동의를 얻기 위한 간편한 장치를 제공하여야 한다. 이용자의 동의 없이 소유, 통제하는 개인정보는 무효화한다. 여기에는 이메일 주소도 포함된다.

나) 뉴욕 : 뉴욕연방법원은 2001년 4월 30일 더블클릭에 대해 프라이버시 침해의 근거가 없다는 판결을 내렸다. 나오미 부치월드 판사는 원고 측은 더블클릭이 도청과 컴퓨터 사기를 금하는 연방법률을 위반했다는 어떤 증거도 제시하지 못했다면서 원고 측 소송을 기각한다고 판결하였다.

6) 논란의 결말

가) 프라이버시 보호론자들과 더블클릭사는 당분간 수집된 정보가 최소한의 기본정보에 그쳐야 한다는 데에 합의하였다. 또한, 개인정보를 분석해 광고에 이용하는 범위도 최소한의 단계에 그치도록 하였다.

나) 더블클릭의 논란은 미국에서의 프라이버시 문제를 새삼스레 각성시키는 계기가 되었고, 정부에서는 프라이버시 보호규정을 만들어야 한다는 자각이 일게 되었다.

다) 시민단체들은 온라인 마케팅 회사들의 개인정보 수집행위나 그 방법, 적용 범위 등을 이용자들에게 구체적으로 알리도록 하는 법률안을 미 의회에 제안할 계획이다.

라) 미국 내 일부 주에서도 온라인 소비자들의 권리를 강화하는 법적 방안을 검토하고 있다.

제3절 유럽연합

1. 유럽연합 개인정보보호 관련 법률의 체계

가. 1981년 조약

유럽연합의 개인정보보호 관련 법률이 미국이나 우리나라의 것과 차이가 나는 것은 공공부문과 민간부문을 단일 법률로 통합하여 규제한다는 점이다. 유럽연합 전체에 통합적인 규율로서 처음으로 체결된 것은 1981년에 유럽회의에서 인준된 ‘개인정보의 자동처리에 관한 개인의 보호에 관한 조약’(Convention for the Protection of Individuals with regard to automatic processing of personal data)이다. 이 조약은 1980년 OECD의 가이드라인이 채택된 직후에 바로 체결되었으며, 정부 및 기업 등에서 컴퓨터 사용이 늘어나고 데이터 처리장비의 이용이 확대됨에 따라 발생할 수 있는 개인의 프라이버시 침해를 방지하고, 개인의 자유와 권리를 보장하는 것을 목적으로 하고 있다. 이 조약은 1981년에 체결되어 1985년이 되

어서야 발효되었는데, OECD 가이드라인에 비해 조약의 형태를 띠고 있음으로 훨씬 더 강한 구속력을 갖고 있다.

나. Directive 95/46/EC of 24. October. 1995

위의 조약을 비준한 국가는 영국, 스웨덴, 스페인, 노르웨이, 룩셈부르크, 아일랜드, 프랑스, 독일, 덴마크, 아일랜드 총 10개국이었다. 조약에 서명은 하였으나 비준을 유보한 국가는 네덜란드를 포함하여 총 8개국이었는데, 이 조약은 서명을 하고 비준까지 완결한 국가에 한해서만 효력이 미치었기 때문에 유럽연합 회원국간의 보호수준이 일정하지 않다는 문제점을 야기하였다. 결국 이로 인한 문제를 극복하기 위하여 1995년 10월 24일에 ‘개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침’(Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data: 95/46/EC of 24 October 1995)이 채택되었다. 이 지침은 물론 1981년에 체결된 조약을 밑바탕으로 하고 있으며 역시 공공부문과 민간부문을 통합하여 규율하고 있다.

1) 목적과 개인정보의 개념

이 지침은 흔히 EU 지침이라고 불리는데, EU 지침의 제 1조를 살펴보면 그 목적을 알 수 있다. 그에 따르면 유럽연합의 회원국들은 자연인의 기본적인 권리와 자유, 특히 그 중에서도 특히 개인 정보처리와 관련한 프라이버시권을 보호해야 하며, 그들은 회원국간 정보의 자유로운 흐름과 교류를 제한하거나 금지할 수 없다. 여기서 ‘개인정보’라는 말이 사용되는데 지침의 제 2조를 살펴보면 ‘개인정보’(personal data)란 정보주체인 자연인을 식별했거나 식별할 수 있는 것과 관련된 모든 정보를 의미하고, 식별가능한 개인(an identifiable person)이라는 것은 신원증명가능 번호 혹은 그의 신체적, 생리적, 정신적, 경제적, 문화적, 사회적 정체성 등을 단일적 혹은 복합적으로 이용하여 그 신원을 파악하는 것이 가능한 사람

을 의미한다. 그리고 정보의 처리(processing of personal data)란 수집, 기록, 조직, 저장, 적용 및 변경, 수정, 복구, 사용, 참고, 사용공개 등 개인정보와 관련하여 그것을 실행하는 작업 또는 작업의 집합을 의미한다.

2) 적용 국가

1981년에 만들어진 조약에 비해 5국가가 더 참여하여 이 조약에 참여하는 국가는 총 15개 국가로서 유럽연합의 회원국 중 독일, 이탈리아, 프랑스, 스페인, 오스트리아, 핀란드, 스웨덴, 룩셈부르크, 벨기에, 아일랜드, 네덜란드, 그리스, 포르투갈, 영국, 덴마크 등이 포함되어 있다. 아이슬란드나 노르웨이 그리고 중앙 및 동유럽 국가들은 적용대상에서 제외된다.

3) 한계와 시사점

따라서 이러한 지침은 회원국들에 대해선 자국법으로 전환하여 관련 문제에 대한 입법을 하는 것을 의무화하지만, 이 조약에 참여하지 않는 국가나 EU이외의 국가에 대해선 직접적으로 영향을 미치지 못한다. 한편으로는 이러한 점이 미국과 갈등을 일으키게 되어 미국으로 하여금 ‘세이프하버(Safe Harbor)’원칙을 만드는 계기가 되었다. 미국은 위에서 언급한 바대로 유럽과 달리 개인정보보호에 대한 법제가 개별법 위주로 되어있는 현실이었고, EU의 지침은 적절한 수준의 개인정보 보호체제를 갖추지 못한 국가로의 개인정보 이전은 엄격하게 제한하였는데(지침 제 25조), 이로 인해 공공부문과 민간부문의 통합이 제대로 이루어지지 않은 미국과 마찰이 생길 수밖에 없었다. 미국 정부는 EU와의 협상을 위해 개인정보보호에 대한 자율규제와 정부규제를 혼합한 세이프 하버원칙이란 접근 방식을 제시하였고, 이중 민간 자율에 보다 무게를 두었다. 세이프하버 원칙은 미국과 EU간에만 적용되는 원칙으로서, 향후 개인정보보호에 대한 법제의 보호 수준이 다른 것 때문에 비슷한 문제가 비롯되는 경우에 있어서 하나의 이정표를 제시해줄 수 있을 것이라 생각된다.

다. 그 후 추가적으로 만들어진 법규로는 정보통신부문에서의 개인정보처리 및 프라이버시 보호에 관한 지침(Directive of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector: 97/66/EC of 15 December 1997)과 정보고속도로에서의 개인정보의 수집 및 처리와 관련한 개인의 보호를 위한 지침(Guideline for the Protection of Individuals in connection with the collection and processing of personal data on information highways: Recommendation No. R(99)5) 등이 있다. 특히 위치정보와 관련해서는 ‘전자통신 부문에서 개인정보 처리와 프라이버시 보호에 관한 유럽연합 지침 2002/58/EC (Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector)’가 있다. 최근 유럽연합에서 제, 개정된 법률을 정리해보면 다음과 같다.

	규범명
규정	• Regulation (EC) No 767/2008 of the European Parliament and of The Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas(VIS Regulation) • Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on community statistics on public health and health and safety at work • Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and

	Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmmes of the Europea Communities
결정	• Commission Decision of 12 December 2007 concerning the implementation of the Internet Market Information System (IMI) as regards the protection of personal data (2008/324/EC) • Commission Decision of 25 March 2008 setting up the 'Platform on Electronic Data Retention for the Investigation, Detection and Proesecution of Serious Crime' group of experts(2008/324/EC) • Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of persnoal data processed in the framework of police and judicial cooperation in criminal matters
권고 및 의견	• Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification(2009/387/EC) • Opinion of the European Data Protection Supervisor on the final report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection(2009/C 128/01)

[표 5-5]

EU에서는 이처럼 공공부문과 민간부문을 종합적으로 규율하는 법규들이 주로 제정되었지만 EU에 있어서도 비식별 개인정보에 대하여 그것의 활용 및 보호에 초점을 맞추어 그 문제를 규율하기 위하여 특정한 법이 입법화된 것은 없는 것으로 보인다. 다만 전 세계적으로 모든 국가의 기업들이 인터넷이나 스마트폰과 같은 온라인 매체를 통해서 소비자들의 구매 성향이나 행태 정보와 같은 것을 수집하여 그들에게 맞춤형 광고를 제공하는 것이 보편화된 현실과 무관하지 않게, EU

에서도 Directive 95/46/EC에 의해 창설된 Article 29 Data Protection Working Party에 의하여 온라인 맞춤형 광고에 대한 의견이 제시되었다.

이 집단에 의해 나온 보고서에서 주장하는 바에 따르면 그들은 온라인 맞춤형 행태 광고가 가져다 줄 수 있는 경제적인 이익에 대해선 전혀 의문을 제시하지 않지만, 소비자의 행태 정보를 수집하여 그것을 그들의 마케팅에 이용하는 일들은 절대적으로 개인의 프라이버시권을 침해해서는 안 되는 것이며 ‘개인의 정보는 보호되어야 한다’는 절대적 원칙의 희생으로 이루어져선 안 된다고 말하면서 미국 FTC보다 강력한 규제의 입장을 띄고 있다. 특히 이용자의 장치에 쿠키를 설치하는 것이나 기타 장치를 통해서 그들의 정보를 수집하는 과정에 있어서는 항상 이용자의 선행적인 명백한 동의가 있어야 함을 강조하고 있고, 이때에도 Directive 95/46/EC는 기본적으로 적용되는 것이기 때문에 이때 언급된 개인정보의 범위도 아직은 식별가능한 개인정보의 범위를 벗어나지 못한 것으로 보인다. 그러나 기업들은 개인 맞춤형 온라인 정보를 제공하기 위해선 이용자들이 방문했던 사이트 등의 정보를 단발적으로 수집하는 것에서 벗어나 한 이용자의 온라인 활동의 굉장히 세부적인 면까지도 다가가서 정보를 수집하게 되므로 이용자로 하여금 명시적인 동의를 받는 절차가 반드시 필요하게 되는 것이고, 이 보고서는 명백한 동의 절차를 받기 위해선 기업들이 정보를 수집한다는 사실 자체가 소비자들에게 투명(Transparency)하게 전달되는 것이 가장 중요하다는 점을 역설하면서 보다 개인정보에 대하여 확실한 규제를 채택하는 것이 그로 인한 피해를 최소화하는데 옳다는 입장을 보인다.

2. 관련 사례들

가. 구글의 Street view에 대한 EU의 제재⁴⁴⁾

구글이 운영하는 ‘스트리트 뷰(Street View)’는 구글 맵, 구글 어스 등에서 사용되는 기술로서 다양한 위치에서 촬영된 한 장소의 풍경들을 360°로 회전해가며 파

44) <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a2Tbh.fOrFB0>

노라마 형식으로 보여준다. 이것은 2007년에 미국의 몇몇 도시에서만 시작된 서비스로서 조금씩 점차 미국 전역 혹은 유럽으로 범위를 넓혀나가고 있다. 그런데 구글의 스트리트 뷰를 통해 제공되는 이미지들이 군사시설의 위치와 그 내부의 풍경까지 보여주는 한편, 미국에선 일광욕을 즐기던 여성의 모습이 노출되기도 하였고, 스트립클럽이나 성인용품 가게에 드나드는 사람의 모습이 찍히기도 하여 개인 사생활에 대하여 심각한 침해의 우려를 낳고 있다.

이러한 논란이 지속되는 가운데 스위스 정부는 ‘스트리트 뷰’가 사람들의 프라이버시권을 침해한다는 것으로 구글을 제소하였다. 아직 스위스를 제외한 나라에서 이와 같은 사안이 공식적으로 문제 제기되어 법원에 까지 제소된 적은 없다.⁴⁵⁾ 특별히 스위스에서 이러한 문제가 먼저 부각이 된 이유는 고객의 비밀 보호가 생명인 은행들이 특별히 많이 모여 있으므로, 금융 비밀 및 고객의 신분 보장 등과 관련한 프라이버시 관련 이슈에 있어서 보다 민감한 위치에 있기 때문에 진행된 일일 것이라 예상된다.

아직 스위스에서도 이와 같은 문제를 정확히 규율할 수 있는 관련 법안이 제정되진 않았는데 스위스의 연방 데이터 보호, 정보 위원회(FDPIC: Federal Data Protection and Information Commissioner)는 스위스 행정 재판소에 법안이 제정될 때까지 구글이 스위스에서 촬영한 모든 사진을 삭제하고 더 이상의 촬영을 할 수 없도록 해달라고 요청하였다. 실제로 이 사건이 스위스 연방 행정 재판소에 제소까지 되게 된 이유에는 예전부터 사람의 개인적인 정보를 담을 수 있는 사진의 촬영에는 엄격한 원칙이 적용되어야 함을 고수하던 FDPIC가 Google에 이러한 문제에 대하여 대책의 필요성을 지속적으로 제기해왔으나 구글이 미온적인 태도를 보였고, 실제로 그 후에 구글의 스트리트 뷰 서비스로 인해 많은 사람의 얼굴이나 자동차 번호판이 그대로 유출되는 사건이 실제로 발생하게 되었기 때문이다.

결국 재판소는 구글이 스트리트 뷰 서비스를 통해 제공하는 이미지가 개인을 식별할 수 있는 정도이며 개인의 프라이버시권을 침해할 수 있는 정도이기 때문에, 서비스를 통해 제공하는 모든 이미지를 제거하라고 지시하였다. 한편 구글은

45) 한편, 우리나라에서는 최근 우리나라에서도 스트리트뷰 서비스를 위해 준비하고 있던 구글코리아의 사무실을 경찰이 개인정보 불법수집의 혐의로 압수수색하여 논란이 제기되고 있다. [\http://news.donga.com/3/all/20100811/30431960/1 참조]

스트리트 뷰 서비스가 실제로 많은 스위스 인들에게 큰 인기를 얻고 있다고 항변하며, 개인이 사생활 침해와 관련하여 문제를 제기할 경우에는 그 해당 이미지를 삭제할 수 있도록 하고 있으며 관련 규제기관과도 이러한 문제에 대해서 항상 논의하고 있으니 큰 문제가 되지 않았기 때문에, 이 서비스 전체에 대해 금지를 내리는 것은 옳지 못하다는 주장이다.

스트리트 뷰 서비스를 통해 제공되는 이미지가 사생활을 침해하는 지에 대해선 스위스 내부에서도 아직 입법화된 것이 없고, FDPIC가 구글을 제소한 이 사건도 최종심까지 가려면 조금 더 시간이 걸리겠지만 스트리트 뷰가 실제로 서비스되고 있는 다른 나라들에 있어서도 같은 문제가 충분히 제기될 수 있기 때문에 스위스 정부에서의 판결이 이러한 유사 관련 문제를 다루는 심판들에 있어선 첫 번째 참고 사례가 될 것이라 예상된다.

한편 EU(European Union's Data Protection Working Party)에서는 구글에게 현재 서비스되기 시작한 후 1년이 지나고 나서야만 삭제되는 사진들을, 촬영되고 서비스 되기 시작한지 6개월 후에 삭제할 것을 권고하였다. 이 문제에 있어서 구글은 사생활 침해 문제가 일어난다면 사진의 이미지를 흐리게 하는 것으로서 대응할 수 있는 것이지 이미지를 제공하는 기간을 줄이게 하는 것은 과도한 억압이라고 대응하고 있다. 구글의 대변인인 Peter Fleischer⁴⁶⁾에 따르면 '흐릿한 이미지'로라도 서비스를 유지하고자 하는 구글의 노력은 합법적이면서도 정당한 것이다. 구글은 이미 공공연하게 12개월의 기간을 선언하였으며 이것이 전 세계적으로도 용인될 수 있는 기간'이라고 주장했다. 이 문제는 아직 공식적으로 법원에 제소된 것은 아니고 EU가 구글에 권고한 것에 그치지만, 향후 비슷한 문제가 지속적으로 발생할 경우 유럽연합 측에서 구글을 제소할 가능성은 높아 보인다.

나. 영국 Phorm 사 사건⁴⁷⁾

영국의 온라인광고업체인 폼(Phorm)사는 온라인에서 소비자의 사용행동을 분석하여 그 소비자에게 맞춤형 광고를 제공하는 Webwise.Discover의 서비스를 제공

46) <http://mashable.com/2010/02/26/eu-google-street-view-order/>

47) <http://news.bbc.co.uk/2/hi/technology/7619297.stm>

하였다. 이것은 소비자의 성향과 행태정보를 수집하는 등 개인의 프라이버시를 침해할 우려가 높다는 이유로 소비자단체들의 반발을 불러일으켰고, 결국 이 서비스를 제공하는 Phorm사는 영국 왕립 검찰청의 조사를 받게 되었다. 그러나 폼 사가 주장하는 바에 따르면 그들은 IP주소나 식별가능한 ID로서 소비자를 식별하여 그에게 맞춤형 광고를 제시하는 것이 아니라, 고객이 사이트에 접속할 때 그에게 랜덤으로 숫자를 부여하고 그 랜덤번호는 소비자의 개인 신상 정보를 저장하지 않고 부여하는 것이기 때문에, 그들은 고객이 누군지 모르면서도 맞춤형 광고를 제시할 수 있는 것인이라, 결국 이 서비스는 온라인상의 개인정보 보호수준을 한 차원 높이면서도 고차원의 서비스 제공을 통하여 인터넷을 진화시킨다고 한다.

결국 이 사건은 EU의 산업 및 기업경영 규제 개혁국(Business, Enterprise and Regulatory Reform-BERR)이 Phorm사는 실제 사이트 방문자의 기록을 계속하여 보관하고 있지 않고, 실제로 보관하는 최소한의 정보가 있다 할지라도 그것은 네티즌을 직접적으로 식별할만한 것은 아니라고 밝혀 Phorm사의 법적 타당성에 대하여 그것이 EU의 테이터법 기준에 충족한다'고 선언하였다. 그러나 고객정보를 조금이라도 수집한다면 그러한 프로파일링 작업에 있어선 언제나 고객이 미리 알아야 하고 사전에 동의하는 방식(Opt-in 방식)을 따라야한다고 주장하였다. 하지만 실제로 이 서비스를 제공하고자 했던 ISP 업체인 BT의 시범 실시에서는 이러한 사전 동意的 단계가 한 번도 이루어지지 않았음을 비평가들은 지적하였고 결국은 이 서비스를 도입하고자 한 BT그룹이 도입을 포기함으로써 사건이 일단락되었다.

제4절 소 결

미국, EU 등을 포함해서 다른 국가에서도 아직 소비자의 행태, 성향 정보나 개인의 위치정보 등 비식별 개인정보를 규율할 수 있는 법규가 마련되어 있지 않은 실정이고, 각 국에서 정의된 개인정보의 개념도 우리나라의 정보통신망 이용촉진

및 정보보호 등에 관한 법률에서 정의된 ‘개인정보’의 개념과 아직은 크게 차이나는 것이 별로 없는 상황이다. 다만 스위스, 영국, 미국 등지에서 일어난 사건을 통해 판단해보건대, 미국과 EU에서도 비식별 개인정보와 관련된 사건들에 대한 법적 고찰을 통해 새로운 입법의 필요성을 살펴보고자 하는 움직임이 관찰되고, 개인정보의 개념을 보다 확장하면서 현행 법률의 적용범위를 넓히고자 하는 노력이 엿보임을 알 수 있다. 실질적으로 비식별 개인정보에 대해서 규제를 하는 법규가 입법화될지에 대해선 장담할 수 없는 일이지만, 각 국가의 이러한 노력들은 개인정보 유출과 관련한 일련의 사건들에 대응을 하면서, 향후 비슷한 문제들이 발생할 경우에 참고가 될 수 있는 지침들을 마련해주고 있다고 할 수 있다.

제6장 비식별개인정보의 보호와 활용에 관한 법정책

제1절 가이드라인

1. 가이드라인의 필요성

현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 해석론으로서, 비식별개인정보는 식별개인정보(이름, 주민등록번호 등의 고유식별자)와 결합하여 개인정보의 묶음 안에 결합되어 있을 경우에 한하여, 그럼으로써 특정 개인을 식별할 수 있게 되는 경우에 한하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제6호의 개인정보에 해당한다고 할 것이다. 이와 달리, 비식별개인정보가 식별개인정보와 결합되지 않은 상태에서, 특정 개인을 식별함이 없이 익명화되어 처리되고 있는 경우에는 현행법상 개인정보에 해당하지 않는다고 봄이 타당하다.

그렇다면, 광고주, 광고회사, 포털사이트 등의 정보통신망서비스 제공자가 개인을 식별함이 없이 비식별개인정보를 수집하는 경우나, 비식별개인정보를 수집한 뒤 이를 나중에 수집한 식별개인정보와 결합하는 경우(Retrospective merge)에 대해서는 현행법상 입법의 공백이 있다는 결론에 이르게 된다. 이는 이러한 경우에 대해서도 자율규제 가이드라인이 마련되어 있는 미국의 경우와 대조되는 것이다.

그러나 고도로 발달된 유비쿼터스 환경에서 비식별개인정보가 가지는 중요성을 감안하면, 이러한 입법의 공백은 정보주체의 개인정보자기결정권과 프라이버시를 심각하게 침해하는 위법행위를 방치하는 결과를 낳게 될 것이다. 다른 한편 인터넷기술과 통신기술의 급속한 발전을 고려해보면, 법률의 제정이나 개정을 통해서 비식별개인정보의 보호를 하는 것도 오히려 이용자의 편익에 반하거나 기업의 효율적인 기술개발 및 시장개척에 커다란 걸림돌이 될 수도 있다. 따라서 본 연구에서는 현행법의 공백을 메우기 위해서 비식별개인정보의 보호에 관해서는 관련 사업자들이 자율적으로 준수할 것으로 요구하는 가이드라인의 제정필요성이 있다는 것을 전제로 하여, 비식별개인정보의 보호와 활용에 관련된 가치들이 조화를 이룰

수 있도록 법정책적 원칙을 제안하기로 한다.

2. 가이드라인의 효력

비식별개인정보의 보호 및 이용에 관해서 방송통신위원회가 가이드라인을 마련하거나 사업자들이 자율적 규범을 마련한다고 해서 그러한 가이드라인이나 자율적 규범이 강제할 수 있는 법률적 효력을 가지고 있는 것은 아니다. 가이드라인이나 자율적 규범을 위반한 사업자에 대해서 법적인 제재를 가할 수 있는 아무런 장치도 없다. 그러나, 기술의 발전에 효율적으로 대응하기 위해서 가이드라인을 제정해서 사업자들이 자발적으로 준수하도록 함으로써 인터넷 및 이동통신사업의 예측가능성을 높이고 소비자들에게 실질적인 보호의 혜택을 제공함으로써 국가 전체적으로 아주 긍정적인 효과를 만들어 낼 수 있는 것도 사실이다. 따라서, 가이드라인의 법적 근거를 관련 법령 내에 마련하는 것이 바람직하다고 생각된다.

제2절 법정책적 제언

1. 개인정보의 범위

현행법은 성명과 주민등록번호와 같이 특정한 개인을 알아볼 수 있는 정보 뿐만 아니라 다른 정보와 쉽게 결합하여 특정개인을 알아볼 수 있는 정보까지 모두 개인정보에 해당된다고 규정하고 있다. 그러나, 어느 정보가 “다른 정보와 쉽게 결합하여 특정개인을 알아볼 수 있는 정보”에 해당되는지 여부는 사업자의 종류에 따라서 그리고 그 사업자의 기술수준에 따라서 크게 좌우되는 문제이다. 뿐만 아니라 인터넷사업자 또는 스마트폰관련 사업자들이 수집해서 맞춤형 광고에 활용하는 상당부분의 정보는 익명처리되어서 현행법상 개인정보에 해당된다고 보기는 어렵지만 어느 순간에 다른 정보와 결합해서 개인정보의 침해로 초래할지도 모르는 잠재적 위험성을 가진 정보들이다.⁴⁸⁾ 따라서, 현행법상 명백히 개인정보에 해

당되는 것은 현행법의 효율적인 운영에 의해서 적절한 보호를 추구하되, 수집단계에서 특정개인을 알아볼 수 있는 비식별개인정보에 대해서도 사업자들이 자율적으로 그 보호에 관한 자율적 규범 내지 가이드라인을 마련해서 보호하도록 노력할 필요성이 절실하다. 비식별개인정보의 보호에 관한 가이드라인의 제정과 준수가 되어야 소비자들도 안심하고 인터넷 및 스마트폰의 이용에 적극적으로 참여할 것이고 기업들도 일정한 기준 하에 미래예측과 투자 및 기술개발을 할 수 있게 되기 때문에 모두의 이익이 되고 국가 전체적으로 부가가치의 생산을 훨씬 높일 수 있게 된다.

사업자들의 자율적인 준수를 유도하기 위해서, 미국 FTC(Federal Trade Commission)는 “온라인 행태 광고에 대한 자율규제 원칙(Self-Regulatory Principles for Online Behavioral Advertising)”을 발표한 바 있고, 우리나라 방송통신위원회도 “온라인 행태정보의 보호 및 이용에 관한 가이드라인(이하 “가이드라인”이라고 약칭함)”을 마련한 바 있다. 동 가이드라인은 “온라인에서 수행한 일련의 활동(웹페이지 방문, 검색, 열람, 구매기록 등)에 관한 정보”를 행태정보라고 규정하면서 그에 관한 보호를 주된 내용으로 삼고 있다. 다만, 동 가이드라인의 행태정보의 개념은 웹브라우저 지문, 위치정보, SNS 관련 정보가 포함되지 않는다고 하는 한계를 포함하고 있지 않는가하는 비판이 제기될 수 있다. 웹브라우저 지문(Web-browser Fingerprint)이라고 함은 사용자의 웹브라우저만으로부터 얻어낼 수 있는 정보로서 웹브라우저 종류 및 운영체제 정보 뿐만아니라 사용자가 사용하고 있는 웹브라우저 플러그인 정보 등을 모두 포함하는 개념으로서 이들을 조합하면 매우 높은 확률로 사용자를 특정할 수 있기 때문에 가이드라인의 행태정보로 보호대상에 포함되어야 하는 것이 아닌가 생각된다. 또한, 무선인터넷이 대중화됨에 따라서 특정 지역의 Wi-Fi 정보를 수집(무선 AP 위치와 MAC address)하여 데이터를 구축하고 단말기 근처에 있는 무선 AP들의 정보를 통하여 단말기 위치를 측정함으로써 온라인이용자들의 위치정보를 파악하고 활용하는 경향이 있다. 따라서, 온라인이용자들의 위치정보도 행태정보의 범위 내에 포함해서 함께 보호해야 할 것으로 생각된다. 특히, 스마트폰 등이 활발히 이용됨에 따라 위치정보가 다른 정보와 결합

48) Federal Trade Commission, Self-Regulatory Principles for Online Behavioral Advertising, pp. 22-23.

하여 프라이버시 침해가 가능하지만 위치정보는 온라인에서 수행한 일련의 활동에 관한 정보는 아니라고 하여 가이드라인에서 제외된다면 현실적으로 상당한 분량의 비식별개인정보가 보호범위 밖에 놓이는 불합리한 결과로 되기 때문이다. 또한, 온라인 및 이동통신상의 소셜 네트워킹 서비스의 경우 이용자의 관계망에 관련된 정보를 바탕으로 맞춤형 광고를 제공하는 것이 가능하다. 특히 최근 페이스북(Facebook)에서는 친구를 맺고 있는 사람들의 선호도를 바탕으로 맞춤형 광고를 제공하기 시작하면서⁴⁹⁾, 이러한 관계망에 관련된 정보의 수집 및 이용 문제가 크게 대두되기 시작하였다. 이러한 이용자의 인간관계망 정보는 자신에 대한 맞춤형 광고에 활용될 뿐만 아니라, 관계망에 등록된 타인에게 행해지는 맞춤형 광고에 사용되는데, 이는 결국 이용자의 “동의를 초과한 정보의 사용”이 아닌가 하는 의문이 제기 될 수 있기 때문에 그에 관한 가이드라인의 적절한 규정이 있어야 할 것으로 생각된다.

2. 온라인 맞춤형 광고의 표시(notice)

개인의 행태정보, 성향정보, 위치정보 등 비식별개인정보를 기초로 하여 온라인 맞춤형 광고를 하는 경우, 광고를 전송하는 제공자는 당해 광고가 정보주체의 비식별개인정보를 활용하여 만들어진 맞춤형 광고임을 표시해야 한다.

이는 정보주체로 하여금, 자신에 관한 어떠한 정보가 수집되는지 알게 하고, 정보수집 및 활용에 대한 거부권을 행사할 수 있도록 기회를 제공하여, 개인정보자기결정권을 실질적으로 보호하기 위한 것이다.

여기에서 어려운 문제는 누가 그러한 의무를 부담하는가의 문제이다. 전술한 바와 같이 광고주, 광고대행사 (즉 온라인 광고 제공자) 그리고 온라인 광고 사이트 제공자가 각각 다른 경우가 많은데 이러한 경우에는 publisher 즉 온라인 광고사이트제공자도 data controller로서의 역할을 하므로 광고제공자와 마찬가지로 의무를 부담한다고 보아야 한다.⁵⁰⁾ 광고대행사와 광고사이트제공자와의 업무분담을 양

49) http://news.cnet.com/8301-13577_3-20010161-36.html?tag=newsLeadStoriesArea.1

50) rticle 29 data protection working party, Opinion 2/2010 on online behavioural advertising, pp11~12

자간 합의를 통해서 해결하면 된다.⁵¹⁾

3. 광고거부권(opt-out) 행사의 기회 제공

비식별개인정보를 활용한 온라인 맞춤형 광고에 대해 정보주체는 자신에 관한 정보의 수집 및 활용을 거부할 수 있는 권리(opt-out)을 가진다고 볼 것이다.

익명화되어 처리되는 비식별개인정보에 대해 정보주체가 사전동의권(opt-in)을 가진다고 보는 것은, 그리고 사전 동의를 얻지 않는 비식별개인정보의 수집 및 활용에 대해 일정한 제재를 가한다고 하는 것은, 광고주의 광고표현의 자유에 대한 과도한 제한이 될 수 있다.

또한, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조 제2항 제1호에 의하면, 이용자가 정보통신서비스를 이용하는 과정에서 생성되는 서비스이용기록, 접속 로그(log), 쿠키(cookie), 결제 기록, 이용정지기록, 페이지뷰 내역, 이용시간대, 검색 사항, 사이트 방문 내역 등의 비식별개인정보는 이용자의 동의 없이 수집할 수 있는 것으로 규정되어 있다. 비식별개인정보가 그 이전에 제공된 식별개인정보와 결합하는 경우(Prospective merge)에도 opt-out으로 규정되어 있는데, 비식별개인정보만이 활용되는 경우에 opt-in을 요구하는 것은 보안수준의 균형을 무너뜨리는 입법이 될 수 있다.

비교법적으로 보아도, 미국의 FTC 가이드라인과 NAI의 자율규제 가이드라인은 비식별개인정보의 수집 및 활용에 관하여 opt-out을 규정하고 있다.

이상의 근거에서, 익명화되어 처리되는 비식별개인정보의 처리와 관련하여 정보주체가 광고거부권(opt-out)을 가진다고 보는 것이 합리적인 법원칙이라고 평가된다. 다만, 현실적으로 facebook과 같이 옵트 아웃 정책을 시행하고 있는 경우에도 인터넷이용자들이 옵트 아웃을 수행하기 위해서 일련의 조작이 복잡한 점은 여전히 현실적인 문제점으로 지적받고 있다⁵²⁾.

한편, 익명화되어 처리된 비식별개인정보가 그 이후에 수집된 식별개인정보와

51) rticle 29 data protection working party, Opinion 2/2010 on online behavioural advertising, p12

52) <http://online.wsj.com/article/SB10001424052748704545004575353092563126732.html>

결합되어 특정 개인에 관한 프로파일로 발전하는 경우(Retrospective merge)에는 정보주체의 프라이버시가 침해될 위험이 높으므로 정보주체에게 사전동의권(opt-in)을 부여하는 것이 타당하다. 정보주체로서는 기존에 수집된 비식별개인정보가 새로이 수집되는 식별개인정보와 결합된다는 사실 자체를 의식하지 못할 가능성이 높다. 자신이 의식하지도 못하는 사이에 자신에 관한 상세한 프로파일 만들어진다면 이는 개인정보자기결정권과 프라이버시권에 대한 중대한 침해로 평가할 수 있다. 따라서 정보통신망서비스 제공자는 정보의 결합에 관한 사실을 이용자에게 고지하고 이용자의 사전 동의를 얻은 후에 비식별개인정보를 식별개인정보와 결합하여 사용할 수 있다고 할 것이다.

4. 광고책임자의 명시

개인의 행태정보, 성향정보, 위치정보 등 비식별개인정보를 기초로 하여 만들어진 온라인 맞춤형 광고를 소비자가 전달받는 경우에 있어선, 소비자가 어떠한 기업이 자신의 정보를 수집하고 관리하고 있는지를 쉽게 알 수 있도록 광고를 전송하는 제공자가 누구인지 광고속에 명확히 표시되어야 할 것이다. 비식별 개인정보를 이용한 광고임이 표시된다 할지라도, 어느 주체가 자신의 정보를 가지고 있는지를 소비자가 알 수 없다면 그것은 ‘개인정보 자기결정권’이 온전히 보장되는 것이라고 할 수 없기 때문이다. 개인정보 자기결정권을 통해 개인들은 자신의 정보가 무단적으로 사용되는 것을 허락하지 않을 수 있을 뿐, 정보가 잘못되었을 경우 잘못된 점에 대하여 정정을 요구할 수 있고, 본인이 원하지 않는 정보에 있어선 삭제도 요청할 수 있다.

이처럼 개인정보와 관련하여 이용자들의 불만을 신속하게 처리하기 위한 정보관리책임자가 지정되어 있어야만 소비자의 정보가 수집되고 취급됨으로 인해 일어날 수 있는 개인정보와 관련된 피해를 최소한으로 줄일 수 있는 여지가 마련된다. 또한 이러한 비식별 개인정보가 도난, 유출, 분실 되었을 경우 그것에 대한 책임을 물을 수 있게 하기 위해서, 그리고 그러한 사실을 사용자에게 지체 없이 통지하고 방송통신위원회에 신고하게끔 하기 위해서라도 광고에 담당 책임자는

반드시 명시되어야 한다.

5. 온라인 맞춤형 광고의 감독기구

비식별 개인정보를 규제하는 법규가 마련이 되고, 기업들이 비식별 개인정보를 이용한 온라인 광고임을 소비자에게 알리고, 사후적으로 광고를 거부할 수 있는 기회를 주고, 기업 내부적으로도 광고 문제와 관련한 책임자를 정한다고 할지라도 그것에 대하여 감독하고, 그 마련된 법규를 실제로 집행할 기관이 존재하지 않는다면 실제로 모든 것이 유명무실화될 가능성이 높다. 온라인 맞춤형 광고와 개인의 정보 유출문제와 관련하여 감독 기구의 설치 없이 기업들의 자발적인 노력에만 문제의 해결을 맡겨놓게 된다면, 기업들의 도덕적 해이(Moral Hazard)가 발생할 가능성이 높으며, 소비자들도 항시 그들의 정보가 잘못 유출될지도 모른다는 불안감 속에서 삶을 살아야 할 것이다. 또한 소비자 정보 유출문제가 발생되었을 때 실질적으로 소비자 들이 구원을 요청할 곳이 없게 되어 그 피해는 고스란히 소비자의 몫으로 남겨지게 되는 것이기 때문에 이는 국민의 기본권으로 지정된 ‘개인정보자기결정권’을 보장하는 길이라 할 수 없다. 감독기구의 마련과 엄격한 법집행 속에 개인정보 유출로 인한 문제의 가능성과 피해 사례를 최소한으로 줄여야만, 상충되는 두 가지 기본권을 규범조화적으로 존중할 수 있는 길을 마련할 수 있을 것이다.

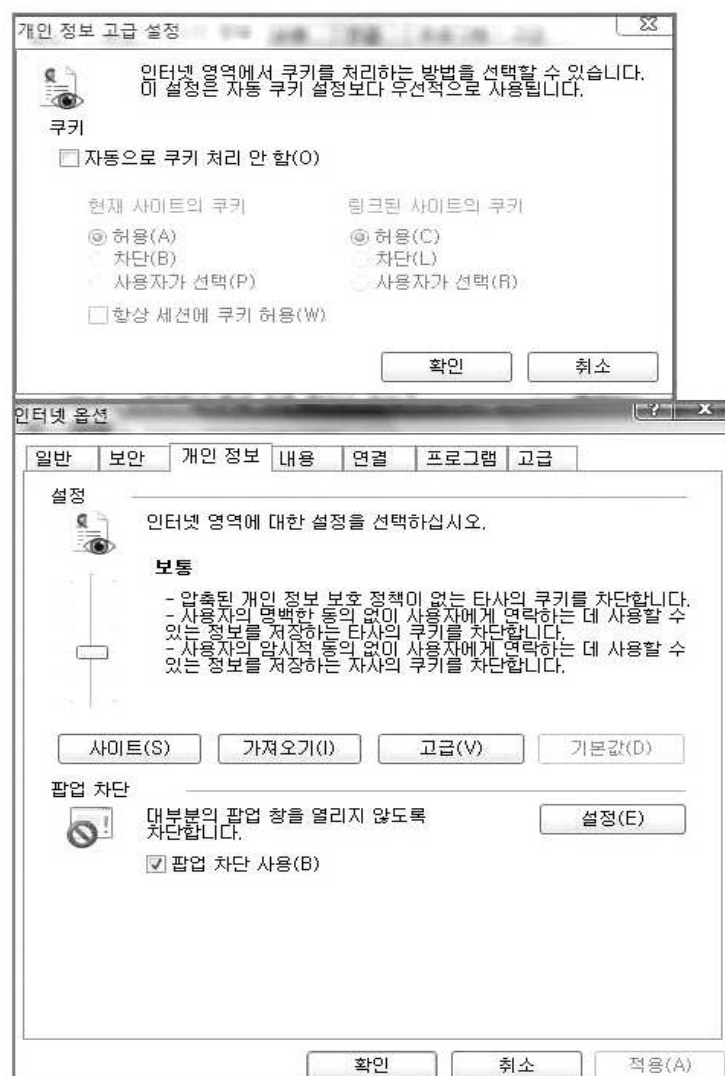
제3절 광고거부권(opt-out) 행사의 구체적 방안

현재 단계에서 활용되고 있는 광고거부권 행사의 방법으로는 다음과 같은 것들이 있다.⁵³⁾ 정보주체가 개인정보자기결정권을 효과적으로 행사할 수 있도록, 광고거부권을 용이하게 행사할 수 있는 방법을 계속해서 연구할 필요가 있다고 본다.

53) 양지연, 2009, 16-17면 참조.

1. 브라우저상의 쿠키 컨트롤

브라우저에서 쿠키를 컨트롤 할 수 있는 방법을 제공한다. 그런데 아쉬운 것은 사용자가 쿠키를 제거하는 순간 제3자가 사용자에게 대한 정보를 수집하는 것을 거절하겠다는 쿠키도 함께 삭제가 되는 기술적인 제한이 있고, 또 사용자가 여러 대의 PC를 사용할 경우 각 PC마다 사용자가 사용자정보 수집을 거절한다는 설정을 하여야 한다는 점이다.



[그림 6-1] 브라우저상의 쿠키 컨트롤⁵⁴⁾

현실적으로는 이용자들이 쿠키를 통해 수집되는 정보가 무엇인지 모르기 때문에 이를 내버려두는 것이 일반적이고, 각각의 서비스에 대하여 선택적으로 행태정보를 제거하는 것이 매우 번거롭다. 또한 최근에는 쿠키 옵션으로 통제가 되지 않는 수퍼쿠키를 이용하여 정보를 수집하는 경우도 빈번하고, 웹브라우저 지문 등 이용자 컴퓨터에는 아무런 정보를 남기지 않고도 수집 가능한 이용정보들이 있기 때문에 단순히 쿠키를 통제하는 현재의 웹브라우저 보안 설정만으로는 충분하지 않다. 따라서 비식별개인정보 수집의 안내 기능을 하는 위젯 등에 수집한 행태정보를 제거하는 기능을 지원하는 추가함으로써 이용자가 수집되고 있는 자신의 행태정보를 쉽게 제거할 수 있도록 지원할 의무를 부과하는 것도 고려해볼 만하다.

2. Windows Live ID 쿠키 셋팅

위의 쿠키삭제와 관련된 불편에 대하여 현재 마이크로소프트가 사용하고 있는 방법은 Windows Live ID 쿠키 셋팅이다. 사용자가 Windows Live ID를 사용하여 로그인한 후 제3자 쿠키를 거절한다는 설정을 해 놓으면 그 Windows Live ID를 사용하여 로그인을 한 이후의 컴퓨터 사용에 대해서는 PC에 상관없이 또한 제3자 쿠키 삭제와 상관없이 사용자에게 대한 정보를 제3자가 수집하는 것을 거절할 수 있다.

3. NAI의 제3자 쿠키 거절 기능

NAI사이트에서는 사용자가 NAI의 멤버 광고 네트워크의 쿠키수집을 한꺼번에 거절할 수 있는 방법을 제공하고 있다.⁵⁴⁾ 사용자가 NAI의 사이트에 접속을 해야 하는 불편이 있기는 하지만 NAI의 멤버들의 제3자 쿠키를 한꺼번에 거절할 수 있다는 편리함이 있다.

54) 출처: 양지연, 2009, 25면

55) <http://www.networkadvertising.org/> (2010.8.26. 방문).

Opt-Out Status

Select all Clear Submit

Network	Status	Opt-Out
aCerno More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
Advertising.com More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
Akamai More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
AlmondNet More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
Atlas More Information	Active Cookie You have not opted out and you have an active cookie from this network.	Opt-Out ☐
AudienceScience More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
BlueKai More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
BlueLithium More Information	Active Cookie You have not opted out and you have an active cookie from this network.	Opt-Out ☐
Collective Media More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
Dedicated Networks More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐
FetchBack More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out ☐

[그림 6-2] NAI의 맞춤형 광고 opt-out 기능⁵⁶⁾

제4절 소 결

비식별 개인정보가 현행 <정보통신망 이용촉진 및 정보보호 등에 관한 법률>에서 언급한 개인정보에 속하지 않는다고 봄이 타당하다면, 현재 한국에는 기업들이 소비자들의 비식별 개인정보를 수집하고 취급하여 이용하는 것과 관련하여 규제할 수 있는 법규가 없는 상태라고 할 수 있다. 비식별 개인정보를 이용한 맞춤형 광고를 규제하는 법규가 공백으로 남아있는 현재 상태가 계속된다면 개인정보침

56) 출처: 양지연, 2009, 22면

해와 관련된 문제가 발생할 것은 명약관화한 일이다. 하루하루가 다르게 발전해나가는 정보통신 환경 속에선 비식별 개인정보라 할지라도 그것이 잘못 사용될 경우 정보주체의 프라이버시와 자기정보결정권을 심각하게 침해할 수 있기 때문에 국가적인 대응이 필요한 시점이라고 할 수 있다.

법정책적으로 몇 가지를 제안하자면 첫째로, 온라인 맞춤형 광고에 있어선 그것이 비식별 개인정보를 사용한 것임을 반드시 밝혀야 할 것이며, 둘째로 정보주체에게 광고를 사후적으로 거부할 수 있는(Opt-out) 권리를 부여하여야 하며, 셋째로 개인정보와 관련하여 발생할 수 있는 소비자들의 불만을 신속하게 해결할 수 있도록 각 기업들은 광고책임자를 정하고 그것을 소비자에게 명시해야하며, 마지막으로 온라인 맞춤형 광고라는 새로운 매체를 감독하고 관리하는 국가적인 기구가 설치되어야 한다.

제7장 결 론

정보 통신 기술이 발달하며 개인정보를 수집하고 활용하는 기술도 점차 다양해지고 있다. ‘개인정보’라는 단어가 활용되는 맥락이 다양해지게 되었으며, 현재 개인정보를 보호하기 위하여 제정되어 있는 법규에서 규정하는 개인정보의 범위를 넘어서 새로운 외연의 개인정보가 등장하게 되었다. 이러한 변화는 프라이버시 혹은 정보 침해와 관련된 문제가 비단 요즘만의 문제가 아니었음을 잘 알고 있음에도, 현대를 살아가는 우리들에게 있어 다시 한 번 개인정보 보호에 대한 필요성을 절감하게 해주는 계기가 되고 있다.

개인정보의 보호가 문제가 된다면 그것을 보호하기 위한 방법으로 가장 쉽게 생각할 수 있는 방법으로는 ‘개인정보’의 무분별한 수집과 가공 및 이용을 엄격히 제한하고, 정보의 유출 자체를 통제해 버리는 방법을 떠올릴 수도 있겠다. 하지만 그것은 정보의 효율적 이용을 막고 궁극적으로는 정보의 이용을 통한 사회적인 효용을 증대시킬 수 있는 길을 원천적으로 봉쇄해버리는 단편적인 대책에 불과할 것이다. 그러한 이유로 인하여 기술이 발전함에 따라 개인정보의 보호를 둘러싼 법적, 정치적, 경제적인 분쟁 사례가 급증할 것이 예측되면서도, 개인 정보의 이용을 원천적으로 제한하는 법규를 만드는 것이 최선의 방법이 아님을 쉽게 짐작할 수 있는 것이다. 실제로 개인 정보의 사용이 효율적으로 이루어질 수 있다면 기업과 소비자의 효용이 증대하는 동시에 보다 큰 사회적 편익이 실현될 수 있다. 따라서 고도로 발달된 유비쿼터스 환경에서 개인정보의 보호와 활용, 두 측면을 조화롭게 달성하는 것이 매우 중요한 과제라고 할 수 있겠으며, 그 중에서도 비식별 개인정보를 어떻게 사용하고 보호해야하는지에 관한 검토 및 제언이 본 연구의 가장 큰 초점이 되었다.

본 연구를 통해선 다음과 같은 사항을 알아보았다.

첫째로, 비식별개인정보의 개념과 유형을 조사하였다. 비식별개인정보는 말 그대로 그 자체로는 특정한 개인을 식별할 수 없는 정보이고, 따라서 익명화되어 처리

되고 있다. 비식별개인정보는 인터넷 사용자의 사이트 접속기록, 서비스 이용기록, 상품 구매내역, 결제기록, 인터넷 접속 시간대 등의 행태정보와 그 사람이 선호하는 방송매체, 신문, 정당, 시민단체, 정치인과 관련된 성향정보, 그리고 IP 주소, 실제 위치 등이 포함된 위치정보, SNS 서비스에서의 다양한 관계정보를 내포하고 있다.

둘째, 개인정보의 보호와 관련된 대한민국 현행법률을 살펴보고, 그 법규들이 문제가 되고 있는 비식별개인정보에 있어서도 적용될 수 있는지의 여부를 살펴보았다. 우선 현행법인 <정보통신망 이용촉진 및 정보보호 등에 관한 법률>이 규정하고 있는 ‘개인정보’는 식별가능한 개인정보임을 우선 알 수 있었다. 그리고 더 나아가 <정보통신망 이용촉진 및 정보보호 등에 관한 법률>의 문언에 대해 문리해석, 체계해석, 역사적 해석, 목적론적 해석 등을 수행한 결과, 위 법률에서는 비식별개인정보를 식별개인정보와 결합하여 특정 개인을 식별할 수 있게 된 경우에만하여 비식별개인정보를 개인정보로 보고 이를 보호하는 것으로 해석된다. 즉, 특정 개인이 식별되지 않은 상태에서 다른 정보와 결합되지 않은 채 익명화되어 처리되는 비식별개인정보는 동 법률에서 규제하는 개인정보가 아닌 것이 되고, 따라서 현행법상으로는 비식별개인정보의 보호와 활용에 대해선 입법의 공백이 존재한다는 결론이 나온다.

셋째, OECD, 미국, EU를 중심으로 외국의 개인정보 보호법제들을 살펴보고, 미국과 EU의 입법례를 통하여 그곳에서도 개인정보와 관련된 법규의 정의는 식별가능한 정보에 한정되어 있다는 점을 찾을 수 있었다. 미국과 유럽에서도 이제야 비로소 비식별개인정보를 이용한 온라인 맞춤형 광고들에 대한 가이드라인을 만들고 있음을 알 수 있었는데, 식별개인정보와 관련해서는 확실한 사전적인 동의(Opt-In)를 받을 것을 요구하고 있었으며, 연구와 관련된 비식별 개인정보의 수집 및 활용에 있어선 사후적으로 수령을 거부(Opt-out)할 수 있는 권리가 소비자에게 필수적으로 주어져야 한다는 공통점을 찾아볼 수 있었다.

넷째, 소비자의 기본권인 개인정보자기결정권과 광고 주체가 향유하는 기본권인 광고 표현자유 원리에 대하여 알아보았고, 그 두 가지의 기본권이 충돌하는 경우에는 양자를 조화롭게 실현할 수 있도록 하는 규범조화적 해석을 시도하는 것이 바람직함을 알아보았다. 실제로 두 개의 기본권 사이에서 우열을 가리어 하나의 기본권을 우선시하고 다른 하나를 배척하는 것은 바람직하지 않다. 비식별개인정보의 개념의 외연을 확정하면서 개인정보자기결정권과 광고표현의 자유, 두 가지의 기본권을 조화롭게 공존하게 하는 것이 연구의 목적인 비식별개인정보의 보호 및 활용이라는 상충되어 보이는 문제에 관한 균형점을 찾는 길이 될 것이다.

다섯째로, 앞의 연구들을 바탕으로 비식별개인정보의 보호 및 활용에 대한 법적책적인 제언을 하였다. 비식별개인정보를 활용한 온라인 맞춤형 광고의 맥락에서 1) 당해 광고가 비식별개인정보에 기초한 광고임을 고지하고, 2) 정보주체에게 광고의 수령을 사후적으로 거부할 수 있는 Opt-out 권리를 부여하고, 3) 광고의 책임자를 명시하여 책임의 소재를 명확히 하고, 4) 온라인 맞춤형 광고라는 시스템 전체를 감독하는 집행기관을 두어야 한다. 이 중의 핵심은 정보주체에게 광고를 거부할 수 있는 Opt-out을 부여하는 것인데, 그러한 권리행사의 상대방 시기, 절차 등의 구체적인 내용은 앞으로 더욱 깊이 연구해야 할 필요성이 있다고 본다.

본 연구는 개인정보의 보호와 관련된 현행 법규에서 정의하고 있는 개인정보란 어떤 것인지를 판단하는 과정을 통하여, 현행법 상으로는 비식별개인정보의 이용과 수집을 규제하는 법규가 존재하지 않는다는 점을 지적함으로써 관련 가이드라인 내지 자율적 규범의 제정을 제안하였다는 점에서 의의를 갖는다. 대한민국의 현실을 직시하는 동시에 외국의 입법례와 가이드라인을 참고해서 보다 명확한 해석론 내지 자율적 보호준칙을 마련할 필요가 있는 것이다. 이를 통해 비식별개인정보의 활용과 보호라는 일견 상충되어 보이는 가치들이 조화롭게 균형을 이루어 나갈 수 있게 된다면, 이는 IT 강국으로서 대한민국이 성장해 나가는데 있어서도 더욱더 커다란 밑바탕이 될 수 있을 것이라고 생각한다. 향후 본 연구결과를 토대로 세미나를 개최함으로써 관련 사업자들과 소비자들의 의견을 수렴해서 방송

통신위원회 및 관련 사업자들이 집행할 수 있는 형태의 가이드라인 또는 자율적
규범을 마련하도록 한다.

온라인 행태정보의 보호 및 이용에 관한 가이드라인(안)

제1장 총 칙

제 1조(목적) 이 가이드라인은 행태정보 기반의 온라인 광고에서 이용자의 프라이버시를 보호하고 안전한 이용환경을 조성하는 것을 목적으로 한다.

제 2조(정의) 이 가이드라인에서 사용되는 용어의 정의는 다음과 같다.

1. “개인정보”란 생존하는 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. “행태정보”란 이용자가 온라인에서 수행한 일련의 활동(웹페이지 방문, 검색, 열람, 구매기록 등)에 관한 정보를 의미한다.
3. “개인 식별성 행태정보”란 행태정보 자체로 개인 식별이 가능하거나 행태정보 보유 사업자가 가진 정보(사업자가 복수인 경우 전체 정보를 의미한다)와 결합하여 개인 식별이 가능한 경우 그 행태정보(이하 “식별성 행태정보”라 한다)를 의미한다.
4. “개인 비식별성 행태정보”란 행태정보 중 식별성 행태정보를 제외한 행태정보(이하 “비식별성 행태정보”라 한다)를 의미한다.
5. “행태정보 기반의 온라인 광고”란 이용자의 행태정보를 수집·축적하여 이용자의 관심에 맞는 광고를 정보통신망을 통하여 제공하는 행위를 말한다.
6. “행태정보 기반의 온라인 광고 제공자”란 행태정보 기반의 온라인 광고를 제공하기 위하여 이용자의 행태정보를 수집·축적·보관·처리·이용·제공·공유·파기 등(이하 “취급”이라 한다)을 하는 자를 말한다.

7. “이용자”란 행태정보 기반의 온라인 광고와 관련하여 취급되는 행태정보의 주체를 말한다.

제 3조(적용범위) 이 가이드라인은 행태정보 기반의 온라인 광고 제공자가 행태정보 기반의 온라인 광고를 제공하는 경우에 대하여 적용한다. 단, 온라인 광고 제공자가 이용자의 행태정보를 2회 이상 취급하는 경우에 한한다.

제2장 행태정보의 수집

제 4조(행태정보 수집 시 고지·동의)

- ① 행태정보 기반의 온라인 광고 제공자가 행태정보 기반의 온라인 광고를 제공하기 위하여 식별성 행태정보를 수집하는 경우에는 당해 이용자에게 다음 각 호의 사항을 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
1. 행태정보의 수집·이용목적
 2. 수집하는 행태정보의 항목
 3. 행태정보의 보유·이용 기간
 4. 이용자가 해당정보를 이용하는 것을 허용 또는 거부할 수 있는 절차
- ② 행태정보 기반의 온라인 광고 제공자가 행태정보 기반의 온라인 광고를 제공하기 위하여 비식별성 행태정보를 수집하는 경우에는 이용자의 동의가 없더라도 행태정보 수집 및 광고를 할 수 있다. 이 경우 이용자가 행태정보의 수집 또는 행태정보 기반의 온라인 광고에 대해 수신 거부 의사를 밝히면 행태정보 기반의 온라인 광고 제공자는 행태정보의 수집 또는 행태정보 기반의 온라인 광고 제공을 즉시 중단해야 한다.

제 5조(행태정보의 수집 제한)

- ① 행태정보 기반의 온라인 광고 제공자는 행태정보 기반의 온라인 광고를

목적으로 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 정보를 수집하여서는 아니 된다. 다만, 제4조제1항에 따른 이용자의 동의를 받은 경우에는 그 정보를 수집할 수 있다.

- ② 행태정보 기반의 온라인 광고 제공자가 행태정보 기반의 온라인 광고를 위하여 행태정보를 수집하는 경우에는 필요한 최소한의 정보를 수집하여야 한다.

제 6조(속이는 행위 등 부정한 방법에 의한 행태정보의 수집 금지) 누구든지 속이는 행위 등 부정한 방법으로 행태정보를 수집하거나 정보를 제공하도록 유인하여서는 아니 된다.

제 7조(아동의 행태정보 수집)

- ① 행태정보 기반의 온라인 광고 제공자가 만14세 미만의 아동으로부터 식별성 행태정보의 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 한다. 이 경우 행태정보 기반의 온라인 광고 제공자는 그 아동에게 법정대리인의 동의를 받기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다.
- ② 법정대리인은 해당 아동의 행태정보에 대하여 제20조에 따른 이용자의 권리를 행사할 수 있다.

제3장 행태정보의 보호

제 8조(행태정보를 이용한 광고 제한) 행태정보 기반의 온라인 광고 제공자는 광고내용이 타인에게 노출되는 등의 과정을 통해 광고 결과가 이용자에게 정신, 신체 또는 재산상의 해악을 미칠 수 있는 경우에는 행태정보를 이용하여서는 아니 된다.

제 9조(행태정보의 보유기간) 행태정보는 행태정보 기반의 온라인 광고를 제공하기 위한 최소한의 기간 동안 보관하여야 한다.

제10조(행태정보의 파기) 행태정보 기반의 온라인 광고 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 행태정보를 지체 없이 파기하여야 한다.

1. 제4조제1항에 따라 동의를 받은 행태정보의 수집·이용 목적을 달성한 경우
2. 제4조제1항에 따라 동의를 받은 행태정보의 보유 및 이용기간이 끝난 경우
3. 사업을 폐업하는 경우

제11조(행태정보관리책임자의 지정 및 책임)

- ① 행태정보 기반의 온라인 광고 제공자는 이용자의 행태정보를 보호하고 행태정보 기반의 온라인 광고와 관련한 이용자의 불만 등을 신속하게 처리하기 위하여 행태정보관리책임자를 지정하여야 한다.
- ② 제1항에 따른 행태정보관리책임자는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제27조 및 동법 시행령 제13조에서 정한 개인정보관리책임자가 겸직할 수 있다.
- ③ 행태정보관리책임자는 행태정보의 도난·누출 등이 발생하지 않도록 필요한 보호조치를 강구하여 시행하여야 한다.

제12조(이용자 대상 정보 제공) 행태정보 기반의 온라인 광고 제공자는 이용자에게 광고의 구현 방법이나 절차에 대해 정확하고 알기 쉬운 정보를 제공할 수 있도록 다음 각 호의 내용을 이용자에게 동영상 등의 다양한 방법으로 알려야 한다.

1. 행태정보 기반의 온라인 광고가 이루어지는 과정과 원리

2. 행태정보 기반의 온라인 광고를 위한 행태정보 수집 대상 웹사이트
3. 식별성 행태정보를 취급하는 경우, 해당 이용자의 권리 행사 방법
4. 행태정보 기반의 온라인 광고에서 활용되는 인터넷 접속정보파일(쿠키) 등의 설치·운영 및 그 거부에 관한 사항

제13조(광고의 표시) 행태정보 기반의 온라인 광고 제공자는 행태 정보를 기반으로 광고를 제공하는 경우 이용자가 쉽게 알아볼 수 있도록 제공하는 광고에 행태정보 기반의 온라인 광고임을 알아볼 수 있는 표시를 명확히 해야 한다.

제4장 식별성 행태정보의 보호

제14조(식별성 행태정보의 이용 제한) 행태정보 기반의 온라인 광고 제공자는 이용자로부터 동의 받아 수집한 식별성 행태정보를 동의 받은 목적과 다른 목적으로 이용하여서는 아니 된다.

제15조(식별성 행태정보의 제공 동의) 행태정보 기반의 온라인 광고 제공자는 식별성 행태정보를 제3자에게 제공하려면 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나가 변경되는 경우에도 또한 같다.

1. 행태정보를 제공받는 자
2. 행태정보를 제공받는 자의 행태정보 이용목적
3. 제공하는 행태정보의 항목
4. 행태정보를 제공받는 자의 행태정보 보유 및 이용기간

제16조(식별성 행태정보의 취급위탁) 행태정보 기반의 온라인 광고 제공자가 제3자에게 이용자의 식별성 행태정보를 취급할 수 있도록 업무를 위탁하는

경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나가 변경되는 경우에도 또한 같다.

1. 행태정보 취급위탁을 받은 자
2. 행태정보 취급위탁을 하는 업무의 내용

제17조(영업의 양수 등에 따른 식별성 행태정보의 이전)

- ① 행태정보 기반의 온라인 광고 제공자가 영업의 전부 또는 일부의 양도·합병 등으로 식별성 행태정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 모든 사항을 인터넷 홈페이지 게시, 전자우편 등의 방법으로 이용자에게 알려야 한다.
 1. 행태정보를 이전하려는 사실
 2. 행태정보를 이전받는 자(이하 “영업양수자등”이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다)·주소·전화번호 및 그 밖의 연락처
 3. 이용자가 행태정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차
- ② 영업양수자등은 식별성 행태정보를 이전받으면 지체 없이 그 사실을 인터넷 홈페이지 게시, 전자우편 등의 방법으로 이용자에게 알려야 한다. 다만, 행태정보 기반의 온라인 광고 제공자가 제1항에 따라 그 이전사실을 이미 알린 경우에는 그러하지 아니하다.

제18조(식별성 행태정보의 보호조치) 행태정보 기반의 온라인 광고 제공자가 식별성 행태정보를 취급하는 경우, 당해 정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 기술적·관리적 보호조치를 하여야 한다.

제19조(식별성 행태정보 분실등의 통지)

- ① 행태정보 기반의 온라인 광고 제공자는 식별성 행태정보의 분실·도난·누출 등이 발생한 것을 안 때에는 지체 없이 해당 이용자에게 통지

하고 방송통신위원회에 신고하여야 한다.

- ② 행태정보 기반의 온라인 광고 제공자는 제1항의 규정에 의한 통지를 하여야 하는 경우에 이용자가 만14세 미만의자인 때에는 이용자 외에 그의 법정대리인에게 알리기 위해 노력하여야 한다.

제5장 이용자의 권리 및 분쟁조정 등

제20조(이용자의 권리 등)

- ① 이용자는 행태정보 기반의 온라인 광고 제공자에 대하여 언제든지 식별성 행태정보의 취급에 대한 동의를 철회할 수 있다.
- ② 이용자는 행태정보 기반의 온라인 광고 제공자에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.
 - 1. 행태정보 기반의 온라인 광고 제공자가 보유하고 있는 식별성 행태정보
 - 2. 행태정보 기반의 온라인 광고 제공자가 식별성 행태정보를 이용하거나 제3자에게 제공 또는 취급을 위탁한 내역
- ③ 행태정보 기반의 온라인 광고 제공자는 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 행태정보를 파기하는 등 필요한 조치를 하여야 한다.
- ④ 행태정보 기반의 온라인 광고 제공자는 제1항에 따른 동의를 철회를 요구하는 방법을 행태정보의 수집방법보다 쉽게 하여야 한다.

제21조(개인정보분쟁조정위원회)

- ① 행태정보 기반의 온라인 광고에서의 행태정보와 관련한 분쟁의 조정을 원하는 자는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제33조제1항에 근거한 “개인정보분쟁조정위원회”에 분쟁의 조정을 신청할 수 있다.

- ② 개인정보분쟁조정위원회는 분쟁조정을 위하여 필요한 자료의 제공을 분쟁당사자에게 요청할 수 있다. 이 경우 그 분쟁당사자는 정당한 사유가 없으면 요청에 따라야 한다.

제22조(기타 사항에 대한 법률 준용) 식별성 행태정보와 관련하여 이 가이드라인에서 규정되지 않은 사항에 대해서는 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 준용한다.

제23조(가이드라인의 개정에 관한 사항) 이 가이드라인은 행태정보 기반의 온라인 광고 관련 기술과 이로 인한 행태정보의 취급방식의 변화에 따라 이해당사자 및 관련 전문가 등의 의견 수렴을 통해 개정할 수 있다.

Abstract

1. Title

Legal review on protection and use of the personally non-identifiable information

2. Purpose of the study

Nowadays the context of using personal information is getting more various after the development in ubiquitous computing technology which is used for collecting and using the personal information data. There are a lot of sensors around us which are collecting people's personal information; besides, online behavioral advertisement which is targeting individual consumers is booming due to the development in the technology of processing collected data.

Thanks to this situation, we can achieve efficient use of the information and the total amount of social welfare(including consumer surplus and producer surplus) is getting bigger. However, the infringement of information owner's privacy, which is resulting from indiscriminating collection and use of personal information, has become a socially serious problem. The scope of this problem is getting various and serious. Unfortunately we can predict that legal, political and economic conflicts concerning protection and use of personal information will increase more.

This study is done for reviewing and analyzing the legal principle of harmonizing two things which seems quite contradictory: protection and use of personal information in the highly-developed ubiquitous environment. In particular, this study mainly focuses on suggesting the principle of using personally non-identifiable information. Previous studies have focused on 'personally identifiable information' including name, resident registration number, e-mail address, etc, which can identify the specified individuals. That is, the main

concern relating to the infringement of personal information is usually about 'personally identifiable information. Furthermore, currently law and policy have already been made and enforced as well as the theoretical research.

What makes us worried is that personally non-identifiable information such as site-access records, service-use records, interesting fields, purchase and payment records, IP address, is also collected for providing targeting-individual service like personally identifiable information(name, resident registration number, e-mail address). This sort of service is typical in the advertising market. Nowadays firms are converting their off-line marketing strategy into the online one and striving to collect personally non-identifiable information such as people's behavior, propensity to consume and location information, which is treated anonymously and cannot identify the information owner by itself, for its efficient marketing. By using this advertising strategy entire social welfare has become larger, for firms can achieve efficient marketing and consumers can be easily given the important and self-important information. At the same time, the problem of abuse and misuse of private information has become more serious and the degree of the damage seems overwhelming.

Nevertheless, it seems that the current law which regulates the personally non-identifiable information is unclear. Whether personally non-identifiable information is included in the scope of 'personal information' which is defined in 'The law of facilitating and protecting the use of Information Network', Article 2, Number 6, is on debate. Besides, substantive and procedural principle which deals the treatment(collection, use, provision) of personally non-identifiable information has not been legislated yet. If the delay of making new regulation about personally non-identifiable information continues, our attempt to find a rational balance between protection and use of personally non-identifiable information will come to fail and social cost from this will grow bigger. Therefore, designing the newly-made law policy concerning the protection and

use of personally identifiable information is considered very urgent and important.

Under the circumstances in which personally non-identifiable information is widely used in the real advertising market, this research reviews the various context of personally non-identifiable information usage and tries to give the law and policy proposal in the context of online behavioral advertisement. We are expecting that this research will become a foundation in the research about information protection and online targeting advertisement and be a good reference for law and policy designing.

3. Contents and scope

The contents and scope of this research are as follows:

- 1) This research investigates the concept and types of personally non-identifiable information and points out that the level of protection of personal information can vary according to the context where the information is used. This is directly related to the interpretation of 'personal information' which is defined in 'The law of facilitating and protecting the use of Information Network', Article 2, Number 6. We will review and check internal and external references about the concept of personal information and raise the problem of which amount of protection is needed in the context of online behavioral advertisement.
- 2) This research will review Korea's law made for protecting the right of self-determination of personal information. Now, Korean information-protection law is divided into two parts: public sector and private sector, and in private sector "The law of facilitating and protecting the use of Information Network" has set a general rule and standard. Whether "The

law of facilitating and protecting the use of Information Network” is applicable will be the first step to determine which law can give criteria for online behavioral advertising. While interpreting laws, it should be considered that personally non-identifiable information can be included in the scope of ‘Personal Information’ by definition.

- 3) This research will provide a comparative law approach about foreign legislation about personal information and personally non-identifiable information. This is for providing an implication from the principles of protection and use of personally non-identifiable information in foreign countries. After checking the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, personal information protection law in U.S, and personal information protection law in EU, we will find an implication by comparing the legislation of U.S and EU.
- 4) This research will provide an overview of the theory of the Constitution concerning the protection and use of personally non-identifiable information. By doing this, we can check which position our Constitution will take on the issue of online behavioral advertisement. This will be a main focus on the regulation on the online behavioral advertisement. Information owner can insist in the right of self-determination of personal information, the right of privacy, the general personal right, property right, and the personal liberty. Among these, the most closely related human rights, however, is the right of self-determination of personal information; thus, we will examine the significance, legal basis, effectiveness, contents, and limitation about it. On the other hand, advertisers can insist on the freedom of speech, the freedom of expression in advertisement, the

freedom of business, property right, and general basic freedom. By the way the freedom of expression in advertisement is the most closely related and highly regulated among these, so we will primarily focus on the constitutional theory about it. As far as online targeting advertisement concerned, the two rights are conflicting each other: information owners' self-determination of personal information and advertisers' freedom of expression in advertisement. The most important thing is to find a normative balance between the two things.

- 5) This research also mainly focuses on setting the borderline that can balance the right of self-determination of personal information and the freedom of expression in advertisement well. If the situation that no special law is made for personally non-identifiable information continues, legal and political conflicts about this will repeat. In order to solve this problem, this research will suggest a legal standard and detailed measures in enforcement.

4. Results of this study

- 1) Personally non-identifiable information is the information that is treated anonymously and cannot identify the specified person by itself. Compared with personally identifiable information such as name, resident registration number, address and sensitive information such as people's thoughts, beliefs, and medical history, personally non-identifiable information gives us less worry about privacy invasion and therefore the level of protection requested by the Constitution is low. However, it is possible that people's privacy will be invaded more easily by using second information derived and synthesized from personally non-identifiable information than by using personally non-identifiable information by itself. Consequently,

higher level of protection should be needed for personally non-identifiable information in the ubiquitous environment that a lot of information is easily gathered and processed.

- 2) If personally non-identifiable information is now treated anonymously and collected and used without identifying specified ones, it cannot be said that personally non-identifiable information is included in the scope of 'personal information' in the law of facilitating and protecting the use of Information Network", Article 2, Number 6. As 'the law of facilitating and protecting the use of Information Network", Article 2, Number 6' is made for protecting the right of self-determination of personal information in the Constitution and it is based on the Article 17(the freedom of privacy) and the Article 10(General Personal Right), it is reasonable that it is existing only to prohibit the invasion of privacy and defamation of characters. Then, it is right to see that this law doesn't regulate the collection and use of personally non-identifiable information which is collected anonymously without identifying a special person. Even though anonymous information were treated, it would be hard to acknowledge that some person's privacy had been violated.
- 3) Analysis of comparative law is centered by OECD guideline on the Protection of Privacy and Transborder Flows of Personal Data of 1980. Foreign countries' legislation of protection of private information is mainly divided into two parts: American law which regulates public and private sector differently, and EU law which regulates both parts together. By comparing the two, we can find out that 'personal information' is defined as 'personally identifiable information' like that of Korean law. As far as online targeting advertisement dealing with

personally non-identifiable information concerned, it is important that ad providers should get the explicit consent from consumers to opt in the collection of personally identifiable information, and the right for consumers to opt out afterwards should be guaranteed for personally non-identifiable information. It is found that those things are common in American FTC guidelines and EU's guidelines.

- 4) It is desired to find a good balance between the two in case that the right of self-determination of personal information and the freedom of expression in advertisement contradict each other. It is not appropriate to put a bigger emphasis on one and to firmly exclude the other, so we are trying to find a balancing-standard interpretation of law, considering the principle of proportion in the Constitutions.
- 5) If it is agreed that the special law for regulating personally non-identifiable information should be essential, it is important to find the equilibrium that can balance the right of self-determination of personal information and the freedom of expression in advertisement. In this research in the context of online targeting advertisement by using personally non-identifiable information,
 - ① It should be notified that this advertisement is based on personally non-identifiable information
 - ② the right for consumers to opt out that advertisement should be provided
 - ③ the person who is in charge of online advertising by using personally non-identifiable information should be specified
 - ④ the institution for monitoring online targeting advertisement should be installed

In our research, what is the most important amongst these is that the consumers must have the right to opt out the advertisement. Furthermore, the details about counterpart, timing and procedure of exercising rights will have to be conducted more deeply afterwards.