방통융합정책연구 KCC-2018-45

개인정보 보호 범위 차등화에 관한 연구

(A Study on the Differentiated Protective Scope of Personal Information)

이성엽/권영준

2018. 12

연구기관 : 한국미래법정책연구소

이 보고서는 2018년도 방송통신위원회 방송통신발전기금 방송통신 융합 정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『**개인정보 보호 범위 차등화에 관한 연구**』의 연구결과보고서로 제출합니다.

2018년 12월

연구기관 : 한국미래법정책연구소

총괄책임자 : 이성엽

참여연구원 : 권영준

목 차

표 목 차

요 약 문

1. 제 목

개인정보 보호 범위 차등화에 관한 연구

2. 연구 목적 및 필요성

빅데이터, 인공지능(AI) 등 4차 산업을 활용한 각종 정보통신기술의 발전에 따라 사업자는 개인정보를 용이하게 수집하고 이를 희망하는 용도로 손쉽게 가공하여 이용할 수 있게 되었고, 개별 이용자에 특화된 서비스를 통해 이용자 편의를 극대화하는 다양한 상품이 출시되고 있다. 그러나 한편으로는, 개인정보의 수집 및 이용 경로가 이전보다 비교할 수 없을 정도로 다양해진 만큼, 정보주체의 부지불식간에 이루어지는 개인정보 오남용 문제 또는 개인정보의 대량 유출 사고 등으로 인한 권리 침해 문제가 국내외를 불문하고 중대한 사회적인 문제로 대두되면서, 개인정보의 보호를 보장하면서도 활발한 이용을 가능하게 하는 규율 간의 조화가 그 어느 때보다 중요한 문제로 부각되고 있다.

그럼에도 불구하고, 현행법은 동의를 비롯하여 개인정보 처리 시 준수하여야 할 각종 의무와 그 요건에 집중하면서, 개인정보의 이용보다는 개인정보의 보호에 규율의 초점이 맞추어져 있다. 나아가 개인정보를 규율하는 국내 법령들은 개인정보의 처리에 따른 각종 의무를 부과하면서도 각 구체적인 의무의 내용에 부합하는 수범 대상을 구분하여 규정하고 있지는 않으며, 또한 '개인정보'라는 단일한 개념을 법 적용의 단위로 사용함으로써 사업자의 입장에서 과연 의무의 대상이 되는 정보의 범위가 어디까지인지 명확하지 않다는 점 역시 개인정보의 원활한 이용을 제한하는 사유로 거론되고 있다.

사업자가 보유하고 있는 정보의 유형별로 규제 준수를 위해 소요되는 비용·인력 등 현실적인 이행가능성이 상이함에도 불구하고, 이와 같은 차이를 고려

하지 않고 규제의 대상 범위를 모두 동일하게 해석할 경우, 사업자에게 과도한 부담을 주거나 이행이 불가능한 의무를 강요하는 결과가 나타나는 반면, 이용자의 실질적인 개인정보 보호에는 도움이 되지 않아 오히려 법의 취지 달성 및 실질적인 집행가능성이 저해될 우려가 있다.

이에 본 연구는 정보통신망 이용촉진 및 정보보호에 관한 법률(이하 “정보통신망법”)상 각종 의무를 기준으로 하여 개인정보의 보호 범위를 차등적으로 해석할 필요성과 그 이론적인 가능성에 대해 먼저 검토하고 방법론 및 차등적인 해석의 결과를 제시함으로써, 사업자들의 현실적인 법령 준수가 가능하면서도 이용자들의 개인정보에 관한 권리가 실질적으로 보장될 수 있도록 하고자 한다.

3. 연구의 구성 및 범위

기존에도 개인정보의 개념 및 관련 규정을 유연화하기 위한 시도는 이루어져 왔으나, 주로 개인정보의 정의 자체를 개정함으로써 문제를 해결하거나 또는 그 외에 가명정보·익명정보의 개념을 새로 도입하는 등 역시 법령의 개정을 전제한 상태에서 개인정보를 활용할 수 있는 방안이 주로 논의되어 왔다. 본 연구는 개인정보의 정의에 대한 법령 개정을 수반하지 않고도 현행법 하에서 균형 있는 해석을 도출하는 방안에 대해 살펴보고자 하였다.

이에 본 연구는 제1장 서론에 이어 제2장에서 개인정보의 보호 범위를 차등적으로 해석할 필요성과 그 이론적 가능성을 서술하고 제3장에서 정보통신서비스 제공자가 수집 또는 생성하는 개인정보의 구체적인 항목과 이를 유형화하는 작업을 선행한 후 제4장에서 유형별로 나눠진 개인정보 의무들에 대한 차등적 해석론을 제시한다.

특히 본 연구는 개인정보 관련 규제의 적정한 보호 범위에 대한 결론을 도출하기 위하여, 각종 입법자료 및 학술 연구 자료의 검토를 통해 헌법상 보장되

는 개인정보자기결정권 또는 정보통신망법상 각 의무 규정이 도입된 배경 및 취지를 종합적으로 분석하였다. 또한 국내법상 개인정보 보호에 관한 기본법인 개인정보 보호법과의 비교, 유사 규정과 그 적용 범위에 대한 해외의 입법례 또는 해석례에 대한 분석을 진행하였다.

4. 연구 내용 및 결과

개인정보 개념의 차등적 해석 필요성에 관한 문제 제기는, 개인정보 관련 법령의 적용과 집행에 있어 현 법제가 개인정보의 보호와 이용 사이에 균형을 잃고 보호에 과도하게 치우쳐 있어, 규제의 범위가 불필요하게 넓게 해석된다는 문제의식에서 출발하였다. 이와 관련하여 본 연구는, 그 근본적인 사유를 개인정보의 개념이 매우 추상적이고 광범위하다는 특성에서 찾고 있다. 이에 따라 개인정보 보호범위의 차등화 필요성에 대한 논의를 시작하면서 개인정보 개념의 모호성에 대해 먼저 지적하고, 아직 장기간에 걸쳐 숙성되지 못한 권리인 개인정보자기결정권의 특성 중 적극적인 통제권적 측면이 필요 이상으로 강조되면서 합리적인 규제 범위 설정에 대한 요구가 고려되지 못하고 있다는 점을 개인정보 개념의 연혁, 타 규제와의 비교 등을 통해 제시하였다. 특히 데이터 수집 및 분석 기술의 지속적인 발전으로 인하여 개인정보의 요소인 식별 가능성은 현실에서 무궁무진하게 확장되어 사실상 개인정보에 해당하지 않는 정보가 거의 존재하지 않는 실정에 이르렀기 때문에, 관련 규제의 핵심적 요건이 “개인정보”라는 단일한 개념으로 설정되어 있는 이상 수범자들은 스스로 법상 의무를 옳게 이행하고 있는지에 대해 더욱 확신하기 어려워져 법적 안정성이 저해되고 있음을 지적하였다.

다만 개인정보의 개념 범위가 추상적이고 모호한 것은 해외의 여러 법령에서도 마찬가지로 발견되는 생래적인 특징으로서, 입법 단계에서 모든 불확실성을 제거할 것을 요구하는 것은 불가능에 가까울 것이다. 결국 개인정보 관련 규제

가 합리성을 확보하고 규제실질화를 이루기 위해 필요한 것은 법률조항의 입법 취지와 전체적 체계, 내용 등에 비추어 의미를 분명하게 하는 해석 작업이겠으나, 그럼에도 불구하고 이와 같은 적극적인 해석 시도가 그간 활발히 이루어지지 못했다는 점을 지적하였다. 나아가 동일한 개인정보의 개념에 대해 동일한 법령 내에서 그 범위를 달리 해석하는 것이 가능한지와 관련하여 법률 해석의 방법론 중 목적론적 해석에 근거한 차등해석의 가부를 검토하였다. 특히 형법을 위시한 타 법령에서 동일한 법개념을 서로 다르게 해석하는 사례를 통해 차등적 해석의 이론적 근거를 검토하였다.

상기와 같은 이론적 가능성에 기초하여, 실제로 개인정보 관련 규제의 적용 범위를 합리적인 범위로 한정할 수 있는 방안에 대해 검토하였다. 먼저 개인정보를 유형별로 분류하였는데, 이론상 개인정보에 대하여는 매우 다양한 분류기준이 소개되고 있으나 연구의 목적에 적합하도록 규제의 적용 범위와 유의미한 관계를 갖는 분류에 초점을 맞추어 소개하였다. 특히 식별성을 기준으로 한 분류에 대해서는, 개인정보의 개념을 모호하고 또한 광범위하게 만드는 핵심적인 요소인 식별 내지는 식별 가능성의 의미에 대하여 사례 등과 함께 자세히 검토하면서, 규제 합리화의 관점에서 식별 가능성 개념의 해석에 있어 중요한 지점은 개인정보가 현재 처리되거나 또는 보관되는 상태를 주요하게 고려하여야 한다는 점을 밝혔다. 또한 다른 정보와의 결합을 통해 개인을 식별할 가능성이 있는 정보(‘개인식별가능정보’)를 현재 개인정보와 결합되어 있는 정보와 그렇지 않은 정보로 나눔으로써, 이후 본 연구의 결론 부분에 해당하는 차등해석 방안의 주요한 기준을 도출하였다. 그리고 개인정보를 수집 출처별, 또는 활용 목적별로도 분류하여 보면서 각각의 분류군에 따라서도 규제를 통한 보호 필요성 수준이 서로 다를 수 있다는 점을 확인하였다.

또한 규제 유형별로 합리적인 차등 해석을 도출하는 작업은 법적인 관점에서 기본권 사이의 충돌 또는 기본권 제한 상황에서 합헌적인 결론을 도출하는 이익형량과정이라는 점을 밝히고, 특히 정보주체의 개인정보자기결정권에 상응하

는 타인의 권리로는 개인정보를 활용하는 기업의 영업의 자유가 있으며, 관련 법령의 해석에 있어서는 영업의 자유 역시 충분히 고려되어야 한다는 점을 기존의 선례와 데이터에 대한 기업의 권리가 점점 더 강조되고 있는 근래의 경향과 함께 제시하였다.

결론 부분에 이르러서는 합리적이고 일관된 해석 기준을 도출하기 위하여 먼저 법령상 각 규제별로 개인정보 자기결정권과 영업의 자유의 비교형량을 통해 어느 정도의 개인정보 보호 수준이 적정한지를 개괄적으로 살펴보았다. 보호조치의무, 동의획득의무, 유출대응의무, 파기의무, 열람제공의무, 이용내역 통지의무 등에 대하여 법제도의 취지를 간략히 검토하며 어떠한 권리가 어떠한 측면에서 우선되어야 하는지를 일별하였다. 각 규제별로 합리적인 해석 방안을 도출함에 있어서는 개인정보자기결정권과 영업의 자유의 충돌이라는 기본적인 틀 안에서, 앞서 도출한 여러 가지 기준을 다양하게 적용하였다. 특히 열람제공요구권에 대응한 사업자의 의무에 관하여서는 개인식별정보와 결합되어 있지 않은 개인식별가능정보의 경우 이용자에게 열람 또는 제공을 허용하기 위하여서는 해당 정보가 어느 정보주체에게 귀속되는지를 확인하여야만 하므로 오히려 개인정보 침해의 위험이 높아지며, 이용자가 권리를 행사한 취지에도 부합하지 않기 때문에 열람제공요구의 대상이 될 수 없다는 결론에 이르렀다. 사업자가 직접 생성하여 내부적 목적에 한하여 활용하는 정보 역시 사업자의 자율 및 영업비밀 침해의 우려 등을 고려할 때 열람제공요구 대상에서 제외되는 것으로 해석할 필요가 있음을 지적하였다. 또한 전 이용자를 대상으로 이루어지는 이용내역 통지에 대해서도 기본적으로 열람제공과 동일한 지적이 가능하며, 특히 이용내역 통지의 방법 측면에서도 개인별로 맞춤화된 내역을 통지할 것을 요구할 근거 또는 실익도 충분치 않다는 점을 다루었다. 그 외에 보호의무, 동의획득의무, 유출대응의무 및 파기의무에 대하여서도 규제의 취지와 실익을 고려한 차등해석 방안을 제시하였다.

5. 정책적 활용 내용

본 연구에서는 개인정보 처리에 관한 주된 의무별로 합리적인 규제 범위 및 내용에 대한 분석 결과를 제시하였다. 이와 같은 차등 해석의 시도는 물론 후속 연구 등의 작업을 통해 이론적 타당성과 설득력을 보다 확보하여야 할 것이며, 사회적 합의를 얻는 과정 역시 필요하다. 개인정보 관련 법령의 해석과 집행에 즉각 반영되기는 어렵더라도, 향후 이와 같은 문제 제기가 누적될 경우 개인정보 보호에 관한 정부 시책에 반영되어 관련 규제기관이 법령에 대한 해설서나 가이드라인을 제작하거나 각종 유권해석을 내림에 있어 근거로 활용될 수 있다.

또한 개인정보에 관한 분쟁 또는 사업자의 법 위반 여부가 문제되는 사안에서 방송통신위원회 등 규제기관이나 수사기관·법원 등은 위법 여부 또는 위법성 수준에 대한 판단을 위한 일응의 기준으로 활용할 수 있을 것이며, 무엇보다 중요하게는 향후 개인정보 관련 법령이 개정되는 경우 축적된 논의를 바탕으로 규제의 적용 범위를 명확히 하거나, 또는 지침과 가이드라인을 통해 구체적인 해석기준을 도입하는 등 입법론 측면에서도 활용가치가 있다.

6. 기대효과

본 연구와 같이 개인정보 관련 규제의 적용 범위를 합리화하려는 시도가 계속하여 축적된다면, 먼저 서비스 제공자로서는 각종 규제에 따라 수범자로서 준수해야 하는 의무의 내용과 범위가 보다 명확해짐에 따라 업무 처리상의 혼란이 감소하고 그간 이용자 또는 이해관계자와의 불필요한 다툼 또는 의견의 불일치 등에 소모되던 비용의 낭비를 막을 수 있다. 또한 개인정보 보호에 관해 보다 명확한 기준을 가지고, 관련 업무 시스템 내지는 매뉴얼을 수립함으로써 이용자 보호에도 더욱 만전을 기할 수 있을 것으로 예상된다.

한편 이용자들로서도 보호받을 수 있는 개인정보의 범위를 보다 명확하게 인

식함으로써 실질적으로 권리 행사에 집중할 수 있게 될 뿐만 아니라, 자신의 개인정보를 생활의 편의 등을 위해 적극적으로 활용하는 정보사회의 한 주체로서 경험하고 있는 불필요한 규제로 인한 불편과 피로를 해소할 수 있다.

궁극적으로는 이와 같은 해석상의 시도가 입법에 반영됨으로써, 개인정보의 보호에 치중한 규제로 인한 사회 전체의 비용 소모가 줄어들고, 나아가 ICT 신산업 시대에 맞는 규제환경을 갖출 수 있게 될 것으로 기대된다.

SUMMARY

1. Title

A Study on the Differentiated Protective Scope of Personal Information

2. Objective and Importance of Research

Due to advancements in various information and telecommunications technologies driven by the fourth industrial revolution such as, big data and artificial intelligence, it has become easily possible for business entities to collect, process and use personal information as the user desires. Through such personalized service to individual users, a wide variety of products that maximize user convenience are being produced. However, with such an unprecedented increase in means to collect and use personal information, privacy infringement due to misuse, abuse and large-scale leakage of personal information occurring without the principals' knowledge has emerged as a serious social issue both domestically and internationally. Under these circumstances, it has become more important than ever before for relevant regulations to strike a balance between the protection and efficient use of personal information.

However, current laws focus more on protecting, than using, personal information and are centered on stipulating various obligations and requirements for processing personal information, including obtaining consent. Moreover, while domestic laws governing personal information impose various

obligations regarding processing of personal information, they fail to specify the applicable scope of each type of obligation. Another limitation to the efficient use of personal information is the lack of clarity for business entities regarding the scope of personal information that falls under the obligation due to the application of a single concept of "personal information" as the basis of enforcement.

In practice, the possibility of compliance varies by type of information retained by a business entity because costs, human resources, etc. required for compliance vary depending on the type of information. Thus, if the applicable scope of the regulations is unified without taking into account such difference, businesses may be faced with excessive burden or non-performable obligation, while failing to adequately protect users' personal information, which could result in undermining practical enforceability and the legislative purpose.

This study first examines the necessity and theoretical possibility of differentiated interpretation of the protective scope of personal information subject to the obligations under the Act on Promotion of Information and Telecommunications Network Utilization and Information Protection, Etc. ("Network Act"), and then provided the methodology and result of such differentiated interpretation so that businesses may practically comply with the relevant laws while guaranteeing the protection of users' rights to personal information.

3. Contents and Scope of the Research

Efforts have previously been made to soften the concept and regulations regarding personal information. However, such efforts predominantly revolved around amending existing laws to revise the definition of personal information itself or to introduce new concepts of "pseudonymous information" and "anonymous information". Instead, this study seeks to identify methods to ensure a balanced interpretation of existing laws without the need to make legislative amendments regarding the definition of "personal information."

To this end, this study begins with an introduction in Chapter 1, followed by a review of the necessity and theoretical possibility of differentiated interpretation of the protective scope of personal information in Chapter 2. This paper will then identify and categorize detailed items of personal information collected and produced by telecommunications service providers in Chapter 3, followed by a proposal for differentiated interpretation of the obligations applicable to each of the categorized personal information in Chapter 4.

In particular, to reach a conclusion regarding the appropriate scope of legal protection of personal information, this study will review a variety of legislative and academic research materials, and comprehensively analyze the factual background and purpose of (i) the provisions for protecting the right to control one's personal information under the Constitution, and (ii) the obligation provisions under the Network Act. These findings will then be comparatively analyzed with the Personal Information Protection Act ("PIPA"), which is the domestic framework law on protection of personal

information, followed by an assessment of similar legislations and their applicable scope of foreign legislations and commentaries.

4. Research Results

The call for a differentiated interpretation of "personal information" originated from the concern that the applicable scope of the relevant regulations is unnecessarily broad due to the unbalance between the protection of personal information and the use of the same in the current legal framework resulting in an excessive inclination towards protection. This study finds that such concern may be attributable to the abstract and broad interpretation of definition of personal information. As such, in discussing the necessity of differentiating the protective scope of personal information, this study first points out the ambiguity of the definition of personal information, and then, based on the history of the concept of personal information and by comparison with other regulations, this study explains that the need for a reasonable scope of personal information regulations failed to be considered due to the overemphasis on the active right to control one's personal information, a right that has not yet had the opportunity to mature over a long period of time. In particular, due to the continuous development of data collection and analysis technologies, the identifiable scope of personal information had substantially broadened to the extent that virtually all information falls under the category of personal information. Thus, as far as the law prescribes a single concept of "personal information" as the key requirement for regulations, business entities subject to regulations will have difficulty in clearly identifying whether they faithfully complied with their legal

obligations, undermining legal stability.

However, such abstract and ambiguous concept of personal information is also inherent in many other foreign laws, and it would be virtually impossible to eliminate all ambiguities in the legislation stage. As such, to enhance the reasonableness and effectiveness of personal information regulations, the meaning of legal provisions should be clearly interpreted in light of their legislative intent and overall structure and purport. However, no such interpretation efforts have been actively made to date. This study then reviewed the possibility of applying teleological interpretation, one of the methods of interpreting legislative provisions, to determine whether a differentiated interpretation of the concept of personal information under the same law is possible. In particular, this study examined the rationale for differentiated interpretation based on the cases of differentiated interpretation of legal concepts in other laws, including, among others, the Criminal Code.

Based on the above theoretical possibility, this study examined how to practically limit the applicable scope of personal information regulations to a reasonable extent. To this end, this study first categorized personal information. Although there are a variety of theoretical classification standards for personal information, only those having significant relevance to the applicable scope of regulations were introduced for the purpose of this study. Particularly, as for the classification standard of identifiability, this study conducted an in-depth analysis of the concept of identification or identifiability along with case examples since this is an essential factor that makes the concept of personal information abstract and broad, and noted that

from a regulatory rationalization perspective, the current processing or retention status of personal information should be given careful consideration in interpreting the concept of identifiability. Also, this study drew out the key standard for method of differentiated interpretation, which falls under the conclusion section of this study, by dividing information which is likely to identify a specific individual when combined with other information ("potentially personally identifiable information") into information currently combined with personal information and information which is not combined. Further, this study categorized personal information by source of collection or purpose of utilization, and confirmed that the appropriate level of protection can vary by such category of personal information.

In addition, this study identified that the process of drawing out a rational differentiated interpretation for each type of regulation is, from a legal perspective, a process of balancing conflicting interests to reach a constitutional outcome in a situation of conflicting or restricted fundamental rights. In particular, this study asserted, along with related precedents and recent trend of growing importance of business entities' rights to data, that businesses' right to conduct business by using personal information is an example of a third party right that correspond to a personal information principal's right to control personal information and accordingly should also be sufficiently considered in interpreting relevant laws.

In the conclusion section, this study briefly reviewed the proper level of personal information protection for each type of regulations by weighing up the right to control one's personal information and the freedom of business

in order to establish a reasonable and consistent standard for interpretation,. The study reviewed the legislative intent behind various obligations including the obligation to take protective actions, the obligation to obtain consent, the obligation to take responsive actions against leakage, the obligation of destruction, the obligation to allow access/provision, the obligation to notify the details of use, and identified which right should take priority from what perspective. In proposing a reasonable interpretation method of each type of regulations, this study employed various standards established as above with the fundamental aim of balancing the right to control one's personal information and the freedom of business. Particularly in relation to business entities' obligation to guarantee users' rights to request for access/produce, this study concluded that the potentially personally identifiable information not combined with personally identifiable information should not be allowed to be accessed by or provided to users, on the grounds that this will require confirmation of the information principal, which would rather increase the risk of privacy infringement thereby ultimately undermining the purpose of the exercise of users' rights. This study also concluded that even information produced and used by business entities for internal purposes should not be allowed to be accessed by and provided to users for the avoidance of possible infringement upon freedom of business and trade secrets of business entities. Further, this study pointed out that the same can be said of the notification made to all users about details of use, and that there are no sufficient grounds or practical benefits for mandating the individualized notification of details of use. In addition, this study proposed methods for differentiated interpretation, that considers the purpose and practical effect of regulations, for the obligation of protection, the obligation to obtain consent, the obligation

to take responsive actions against leakage and the obligation of destruction.

5. Policy Suggestions for Practical Use

This study analyzed and proposed a reasonable scope and details of regulations for each type of major personal information processing obligation. The proposed differentiated interpretation should be improved in terms of its rationality and legitimacy through follow-up studies, and should also be generally accepted in society. Albeit not immediately reflected in interpreting and enforcing personal information laws, if the above issues continue to be raised, the proposed interpretation would serve as a basis for governmental policy for personal information protection and of regulatory authorities' interpretation, guidelines and authoritative ruling in the future.

In addition, the proposed interpretation would also serve as a basis for regulatory agencies (e.g., Korea Communications Commission), investigative agencies, courts, etc. to find illegality and determine the degree of illegality in disputes over personal information or in a case involving the alleged violation of personal information law by a business entity. Above all, it would serve as a useful tool from a legislative perspective such as clarifying the applicable scope of regulations based on accumulated discussions in case of amendments to personal information laws, or establishing specific interpretative standards through guidelines.

6. Expectations

If this study is followed by continued efforts to rationalize the applicable scope of personal information regulations, service providers subject to regulations would be able to clearly recognize the details and scope of their obligations and thus could avoid confusion in conducting their business and save costs arising from unnecessary disputes or conflicts with their users and other interested parties. They would be also able to establish clearer standards, business system and manual for personal information protection and thus be more fully committed to protecting users.

In addition, users would be able to have a clearer knowledge about the protective scope of their personal information allowing a more effective exercise of their rights., Users, as members of information society, can also avoid inconvenience and annoyance arising from unnecessary regulations on the personal information they provide for convenience.

Ultimately, if reflected in future legislation, the proposed interpretation would reduce overall social costs incurred from the regulations weighted towards protection of personal information, and would contribute to establishing a more fitting regulatory environment for ICT industries.

CONTENTS

제 1 장 서 론

현대 산업활동이 인터넷을 중심으로 재편되는 과정에서 개인정보의 이용의 규모와 폭이 이전에 비하기 어려운 수준으로 증대되었고, 국가와 기관, 기업이 운영하는 개인정보 데이터베이스가 무수히 존재함에 따라 자연히 개인정보 침해 또는 유출의 문제가 더욱 빈발하면서 개인정보 침해 문제가 대두되었다. 이에 따라 개인정보 보호에 관한 법적 논의 역시 개인정보자기결정권 등의 권리 침해를 효과적으로 예방할 수 있는 방법에 초점을 맞추어져 왔다. 개인정보의 보호에 관한 일반법인 「개인정보 보호법」, 정보통신서비스 이용자의 개인정보보호에 관하여 규정한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법")」, 금융거래 등 상거래 당사자의 신용정보 보호에 관하여 규정한 「신용정보의 이용 및 보호에 관한 법률」 등은 모두 이러한 배경하에서 제정된 것이다.

그러나 근래 빅데이터 기술, 기계학습에 기반한 인공지능 기술이 "4차 산업혁명"이라 통칭되는 산업구조의 대대적인 변화 현상을 촉발함에 따라 개인정보를 포함한 디지털 정보의 효율적인 이용을 촉진하는 것이 그 어느 때보다도 중요하게 되었다. 이에 따라 이용자의 사생활을 존중하고 개인정보 자기결정권을 보호하면서도, 이를 침해하지 않는 범위에서 사업자로 하여금 개인정보를 최대한 활용할 수 있도록 하기 위한 법적·제도적 차원의 논의가 전세계적으로 이루어지고 있다.[1)]

반면 우리나라에서는 아직 위와 같은 개인정보 활용의 중요성이 충분히 부각되지 못한 측면이 있고, 이로 인하여 개인정보 관련 법령과 정책에도 규제 시

1) Elisa Bertino & Elena Ferrari, "Big Data Security and Privacy", 31 Studies in Big Data (2017); European Data Protection Supervisor, "Meeting the challenges of big data", Opinion 7/2015 (2015); Yolande Berbers et al., Privacy in an Age of the Internet, Social Networks and Big Data, Royal Flemish Academy of Belgium for Science and the Arts (2018) 등 참조.

행에 수반되는 사회·경제적 비용에 관한 고려가 충분히 반영되어 있지 않다. 특히개인정보 관련 법령들이 수범자에게 요구하는 의무의 내용을 합리화하려는 시도가 이 충분히 합리화되어 있지 않다는 점을 들 수 있다. 각 수범자가 다루는 정보가 개인정보에 해당하기만 하면, 해당 정보의 생애주기에 따라서 “개인정보”를 세부적으로 유형화하여 정의하고 있지 아니하다는 점에서 여실히 드러난다. 현행 개인정보 관련 법령들은 개인정보를 일반개인정보, 민감정보, 주민등록번호 정도로만 구별하고 있을 뿐이다. 이로 인하여 각 법령들이 그 수범자인 사업자에게 부여하고 있는 각종 의무의 내용과 범위를 해석함에 있어서 사업자가 처리하는 개인정보의 유형 및 그에 따른 보호필요성의 정도를 반영하기가 어렵게 되어 있다.

그러나 법령상 ‘개인정보’라는 단일한 용어가 사용되었다는 이유만으로 보호의 대상이 되는 개인정보의 의미 및 범위를 모두 동일하게 해석하는 경우에는 사업자에게 과도한 부담을 주거나 이행이 불가능한 의무를 강요하는 결과가 된다. 이는 개인정보의 효율적인 활용을 저해하는 반면, 이용자의 개인정보를 보호하는 데에는 실질적인 도움이 되지 않는다. 따라서 규제별로 그 적용 대상이 되는 개인정보의 범위를 탄력적으로 볼 수 있는지 여부에 관한 새로운 견해 및 연구 결과의 제시가 필요하다.

이하에서는 ‘개인정보의 안전한 활용’에 초점을 맞추어 개인정보 규제에 대한 새로운 접근을 제시하기로 한다. 법체계상 개인정보 보호에 관한 일반법은 개인정보 보호법이나, 실무상 개인정보 보호와 관련된 문제들은 인터넷 등 정보통신망을 이용한 대량의 개인정보 수집·이용 과정에서 발생하고 있다. 4차 산업혁명이 정보통신 기술을 기반으로 이루어지는 것인 만큼, 앞으로는 개인정보 보호 문제에 있어 정보통신망법 상 규제의 중요성이 더욱 증대될 것이다. 따라서 이하에서는 정보통신망법 상 개인정보 보호 관련 규제들 중심으로 논의를 전개하기로 한다.

가장 먼저 개인정보의 보호 범위를 차등적으로 해석할 필요성과 그 이론적

가능성을 살펴보고(제2장), 정보통신서비스 제공자가 수집 또는 생성하는 개인정보의 구체적인 항목과 이를 유형화하는 작업을 선행한 후(제3장), 유형별로 나눠진 개인정보 의무들에 대한 차등적 해석론을 제시한다(제4장). 특히 본 연구에서는 개인정보 관련 규제의 적정한 보호 범위에 대한 결론을 도출하기 위하여 각종 입법자료 및 학술 연구 자료의 검토를 통해 헌법상 보장되는 개인정보자기결정권 또는 정보통신망법상 각 의무 규정이 도입된 배경 및 취지를 종합적으로 분석하였다. 또한 국내법상 개인정보 보호에 관한 기본법인 개인정보보호법과의 비교, 유사 규정과 그 적용 범위에 대한 해외의 입법례 또는 해석례에 대한 분석을 진행하였다.

제 2 장 개인정보 보호범위의 차등화 필요성

제 1 절 개인정보 개념의 모호성

1. 개인정보 개념의 정립 및 법제화

가. 개념의 발전 과정

개인정보에 관한 권리가 처음 법적인 개념으로 정립되기 시작한 것은 1888년 미국의 전직 미시간주 대법원장 Thomas Cooley가 법관 퇴직 후 작성한 논문에서 “홀로 있을 권리(the right to be let alone)”의 개념을 제안한 시점으로 평가된다.[2] 신체의 안전에 속하는 여러 권리 가운데 하나인 인격의 불가침성에 속하는 것으로 주창된 “홀로 있을 권리”는 타인의 권리에 간섭하지 않는다는 소극적 권리로 시작되었으나, 논의가 발전해 감에 따라 보다 적극적 관점에서 프라이버시를 이해하려는 시도가 이어졌다. 그 중 대표적으로 언급되는 학자 중 하나인 Charles Fried는 저서 “Privacy”에서 “프라이버시란 우리들에 관한 정보의 부재(不在)만을 의미하는 것이 아니라 우리 자신에 관한 정보를 우리 스스로가 통제(統制)하는 것을 의미한다”고 역설했다.[3]

이와 같이 사생활의 비밀 내지는 자유와 유사한 소극적 개념으로 이해되던 프라이버시는 1965년 미국 연방대법원이 Griswold v. Connecticut, 381 U.S. 479 사건에서 피임약의 사용을 제한하는 코네티컷 주법을 “은밀한 결정(intimate

---

2) Thomas Cooley, Law of Torts(2nd ed.), Chicago: Callaghan & Co. (1888), 최경진, “잊혀질 권리 – 개인정보 관점에서”, 정보법학 제16권 제2호(2012), 101에서 재인용.

3) Charles Fried, "Privacy", 77 Yale Law Journal 475, 482 (1968), 한국언론재단, 개인정보보호와 언론(2008), 80에서 재인용.

decision)을 할 권리"를 침해하여 위헌이라고 선언함으로써 미국에서는 헌법적 권리로 격상되기에 이르렀다. 나아가 1977년 연방대법원은 Whalen v. Roe, 429 U.S. 589 사건에서 프라이버시권에 관해 설시하면서 ① 자신의 중요한 문제에 대해 자율적이고 독자적으로 결정을 내리고자 하는 이익 및 ②사적인 사항이 공개되는 것을 원치 않는 이익을 포괄한다고 정의하여, 개인정보에 대한 정보주체의 통제권으로서의 "정보프라이버시(informational privacy)" 개념이 비로소 공식적으로 인정되기에 이르렀다.[4)]

한편 우리나라의 경우에도 1980년대 후반부터 학계에서 개인정보 보호법제의 도입이 필요하다는 취지의 주장이 다수 제기되었고,[5)] 정부 및 국회에서도 이에 부응하여 1994. 1. 7. 「공공기관의개인정보보호에관한법률」을 제정(1995. 1. 8. 시행)하면서, 정의 조항에서 '개인정보' 개념을 아래와 같이 최초로 규정하고 국가와 지방자치단체 및 일부 공공기관이 이를 보호할 의무를 마련하였다.

<표 2-1> 공공기관의 개인정보에 관한 법률의 개인정보 정의 규정

「공공기관의개인정보보호에관한법률」[법률 제4734호, 1994.1.7. 제정, 1995.1.8. 시행] 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 2. "개인정보"라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 情報만으로는 특정개인을 識別할 수 없더라도 다른 情報와 용이하게 結合하여 識別할 수 있는 것을 포함한다)를 말한다.

4) 김현경, "개인정보보호제도의 본질과 보호이익의 재검토", 성균관법학 제26권 제4호(2014).

5) 이경호, "정보화사회에 있어서 프라이버시권의 보호: 개인정보처리에 관한 프라이버시권의 법적 보호를 중심으로", 박사학위논문, 동국대학교(1986); 황우여, "개인정보보호법. 정보공개법(시안)", 고시계(1989); 이준구, "개인정보의 보호", 법학논거(1991); 최호준·안황권, "개인정보보호에 관한 연구", 경기행정논집(1991) 등 다수

또한 대법원은 1998. 7. 24. 국가보안사령부가 과거 민간인을 상대로 개인정보를 수집 및 관리한 행위의 불법성을 판단하면서 “헌법 제10조의 행복추구권과 헌법 제17조의 사생활의 비밀과 자유에 관한 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장”하기 위함이라고 판시하면서 정보주체의 개인정보에 대한 통제권의 헌법적 배경을 제시하였다.[6]

여기에 더해 헌법재판소는 2005. 5. 26. 열 손가락의 회전지문과 평면지문을 날인하도록 정하는 주민등록법 규정의 위헌성을 판단하면서 ‘개인정보자기결정권’이라는 기본권을 처음 제시하고, 이를 독자적 기본권으로써 새로이 헌법적으로 승인한다고 명시적으로 밝힌바 있다. 여기서 헌법재판소는 ‘개인정보자기결정권’을 “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”라고 정의하고, “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 포함”한다고 하였다.

또한 헌법재판소는 “현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치”가 바로 개인정보자기결정권이라고 판시하였으며,[7] 이후 개인정보자기결정권이라는 개념은 대법원 결정문 및 판결문에도 수

---

6) 대법원 1998. 7. 24. 선고 96다42789 판결.

7) 헌법재판소 2005. 5. 26. 선고 99헌마513, 2004헌마190(병합) 결정, 헌법재판소 2005. 5. 26. 선고 99헌마513 결정 등.

용되었다.[8)]

한편 국회는 2001. 1. 16. 「정보통신망이용촉진등에관한법률」을 전부개정(2001. 7. 1. 시행)하면서 법률의 명칭을 「정보통신망이용촉진및정보보호등에관한법률(이하 "정보통신망법")」로 변경하고 법률 내에 정보통신서비스이용자의 개인정보의 보호제도에 관한 규정을 대폭 추가함으로써 그간 국가와 지방자치단체 및 일부 공공기관에만 인정되던 개인정보 보호의무를 민간 정보통신서비스제공자에게 확대하였고, 그로부터 10여년 후인 지난 2011. 3. 29.에는 개인정보 보호에 관한 일반법인 「개인정보 보호법」을 제정(2011. 9. 30. 시행)하는데 이르렀다. 국내 법령 역시 1994년 공공기관의 개인정보 보호에 관한 법률 제정 당시부터 개인정보의 열람 또는 정정을 요구할 수 있는 권리에 관한 규정을 두고, 2001년 개정 정보통신망법에 처리 목적을 달성한 개인정보의 파기 의무 등을 두면서 '적극적인 통제권'으로서의 개인정보자기결정권을 법제화하였다.

즉 개인정보 보호법제는 "홀로 있을 권리(the right to be let alone)"라는 최초의 출발점에서 알 수 있듯이 외부로부터 방해 받지 않을 소극적 권리에서 출발하였으나, 현재는 국내외를 불문하고 정보주체에게 그 정보에 대한 적극적인 통제권이 있음을 전제로 이를 충분히 행사할 수 있도록 보장하는 적극적 권리로 확장되어 왔다.

나. 적극적인 통제권의 의미 및 범위

현대의 개인정보 개념이 지금에 오기까지 거쳐 온 논의와 발전 과정을 살펴보면, 그 법적인 의미가 비근한 예를 찾기 어려울 정도로 단시간에 크게 확장 및 발전된 것을 알 수 있다. 신체나 재산 등이 당연히 개인의 권리의 대상으로 여겨져 왔던 아주 오랜 시간 동안 개인정보는 그 개념조차 인식하기 어려웠을

8) 대법원 2011. 5. 24. 자 2011마319 결정, 대법원 2014. 7. 24. 선고 2012다49933 판결 등.

정도로 ‘개인정보가 무엇인지’에 대한 논의조차 충분히 이루어지지 못한 상태였으나 최근에는, 특히 인터넷의 급속한 발전과 함께 그 개념에 대한 논의가 활발히 이루어지고 있다. 또한, 19세기에 가까워지고 나서야 “홀로 있을 권리”라던가 “은밀한 결정을 할 권리” 등으로 모호하게 등장하였던 개인정보 관련 권리가 지금에 와서는 개인정보자기결정권이라는 헌법재판소가 인정하는 적극적인 통제권으로 자리잡았다. 인격권에 기초하여 헌법적인 가치를 인정받은 유사한 권리들인 신체에 관한 자기결정권이라던지, 성적 자기결정권, 일반적 행동의 자유 등에 비할 때, 제3자의 자유의사에 기한 행위를 제어할 수 있는 적극적인 권리로 인정받게 된 것이다.

이와 같이 개인정보에 관한 권리의 성격은 ‘알려지지 않을 권리’라는 소극적 형태에서부터 출발하여, 누구에게 알려질지를 직접 결정하는 것에서 더 나아가 불특정한 제3자에게 알려질 가능성을 차단하기 위해 정보처리자의 작위의무까지도 발생시킬 수 있는 통제권으로 넓혀져 왔다. 그러나 권리의 성격은 소극적인 불간섭권의 성격에서부터 적극적인 요구권에 걸쳐 있는 것에 비해, 보호대상은 ‘개인정보’라는 단일한 대상으로 귀결되고 있다. 개인의 핵심적인 자유영역에서는 기본권 제한이 엄격한 조건 하에서 가능한 반면, 사회적 연관성과 기능이 클수록 광범위한 제한이 가능하다는 기본적인 기본권 법리에 비추어보면, 타인의 작위의무를 발생시키는 적극적인 권리는 통상적으로 보호영역이 비교적 축소되기 마련이다. 헌법이론상 소극적 성격과 적극적 성격을 동시에 갖고 있는 것으로 풀이되는 또 다른 예인 알 권리를 보더라도 그렇다. 정보를 국가 등의 간섭과 방해 없이 받아들일 수 있어야 한다는 소극적인 알 권리 대상으로서의 정보와, 적극적인 정보 수집 및 요청권 대상으로서의 정보 범위가 서로 같을 수는 없다. 실제로 후자가 입법을 통해 구체화된 “정보공개청구권”의 경우, 대상이 되는 ‘정보’의 범위는 공공성이 매우 높은 것으로 한정된다.

헌법적 개념 또는 보호법익은 대체로 추상성이 매우 높으므로, 이를 법제도

로 구체화하는 데에는 다양한 방법이 사용된다. 예컨대 앞서 예시로 든 정보공개청구권을 법제화한 공공기관의 정보공개에 관한 법률에서는 비공개대상정보를 상세하게 정하고 있으며(제9조), 제3자의 비공개 요청 등으로 권리 범위를 합당하게 하는 장치를 구현하고 있다(제21조). 또한 표현의 자유의 경우 보호의 대상인 '표현'이 언론, 출판, 집회, 결사 등의 다양한 실체적 개념으로 분화하여 보호필요성의 수준에 맞도록 구성된 개별 법률의 보호를 받는다. 쾌적한 생활을 할 권리를 위해 보호받아야 할 일조권의 경우 일응의 객관적 기준이 필요하다는 판단 또는 어느 정도의 사회적 합의가 이루어져, 법령상[9] 또는 판례상[10] 정량적인 수치기준이 제시되고 있기도 하다.

그러나 적어도 국내법상으로 한정하여 볼 때, 개인정보의 경우는 그렇지 못하다. 개인정보자기결정권이라는 헌법상의 추상적인 용어가 거의 그대로 쓰이면서, 법상 개념이 구체화되어 있지도 않고, 일부의 규제유형에 대해 좁은 범위의 예외만이 인정되어 있다.[11] 특히 개인정보 파기나 열람·제공, 이용내역 통

9) 건축법 시행령 제86조

> 제86조(일조 등의 확보를 위한 건축물의 높이 제한)
> ① 전용주거지역이나 일반주거지역에서 건축물을 건축하는 경우에는 법 제61조제1항에 따라 건축물의 각 부분을 정북(正北) 방향으로의 인접 대지경계선으로부터 다음 각 호의 범위에서 건축조례로 정하는 거리 이상을 띄어 건축하여야 한다.
> 1. 높이 9미터 이하인 부분: 인접 대지경계선으로부터 1.5미터 이상
> 2. 높이 9미터를 초과하는 부분: 인접 대지경계선으로부터 해당 건축물 각 부분 높이의 2분의 1 이상

10) 대법원 2007. 9. 7. 선고 2005다72485 판결 등

> 아파트와 같은 공동주택의 경우 동지를 기준으로 오전 9시부터 오후 3시까지 사이의 6시간 중 일조시간이 연속하여 2시간 이상 확보되는 경우 또는 동지를 기준으로 오전 8시부터 오후 4시까지 사이의 8시간 중 일조시간이 통틀어 4시간 이상 확보되는 경우에는 일응 수인한도를 넘지 않는 것으로 보아야 한다.

11) 개인정보 보호법의 경우, 그 범위가 한정적이기는 하나 규제의 실질화를

지와 같이 타인의 적극적인 작위의무를 전제로 한 규정에서도 권리의 성격에 부합하게 합리적으로 의무범위를 제한하기 위한 예외규정이나 해석기준 등이 적합하게 제시되어 있다고 보기 어렵다.

<표 2-2> 정보통신망법상의 예외 인정 규정

제22조(개인정보의 수집·이용 동의 등) ② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다. 1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우

위하여 개인정보 또는 개인정보 처리의 범위 중 일부에 대해 법 적용을 명시적으로 배제하고 있다.

개인정보 보호법 제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다. 1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보 2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보 3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보 4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보 ② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다. ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우 제29조(개인정보의 파기) ① 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보를 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.

인권 개념이 정립되고 개인의 인격을 보다 넓게 보호해나가는 과정에서 등장한 개인정보에 관한 권리 개념과 법 제도는, 국가의 감시와 정보 수집, 언론에 의한 무분별한 정보의 노출에서 나아가 다양한 이익집단에 의한 악용 또는 무단 사용을 겪어나가면서, 개인정보 처리를 위해서는 이용자로부터 동의를 받아야 한다는 기본적인 형태만이 아니라 이용자의 개인정보자기결정권을 실질적으로 보장하기 위한 다양한 형태의 의무들을 마련하기에 이르렀다. 그럼에도 불구하고 개인정보의 개념범위는 그에 발맞춰 적절히 정립 또는 재단되지 못하고, 오히려 아래에서 설명하는 것과 같이 기술의 발전에 따라 계속하여 무한히 확장되고 있는 실정이다. 또한 기업의 무분별한 정보 활용이나 상업적 이용 행태만이 부각되면서, 개인이 더 이상 수동적인 감시 또는 관찰의 대상이 아니라 적극적으로 정보를 제공하며 서비스를 이용하는 주체라는 측면은 간과되고 있기도 하다.

이에 본 연구서에서는 해석론을 중심으로 흔히 통제권이라고 표현되는 개인정보에 관한 권리의 적절한 범위 또는 그 범위 설정의 방법 내지 기준에 대하여 논하고자 하며, 아래에서는 구체적으로 문제되는 지점이 무엇인지부터 짚어보며 살펴보도록 하겠다.

2. 추상적 법개념으로 인한 법 적용상의 난점

가. 국내외 법령상의 개인정보에 대한 정의

정보통신망법의 개인정보의 정의에는 그 자체로 '개인을 알아볼 수 있는 정

보'(개인식별정보) 및 '다른 정보와 쉽게 결합하여 알아볼 수 있는 정보'(개인식별가능정보)가 별도의 구분 없이 병렬적으로 포함되어 있다. '식별가능성' 개념을 기반으로 한 이와 같은 정의 방식은 현재 개인정보 보호법 및 신용정보의 이용 및 보호에 관한 법률에서의 각 정의 규정에서도 마찬가지로 발견되는바 이는 국내의 개인정보 보호법제의 일반적인 특성이라 할 것이다.

<표 2-3> 국내 개인정보 관련 법령상 개인정보 정의규정

정보통신망법상의 정의규정
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 6. "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.

개인정보 보호법상의 정의규정
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

신용정보의 이용 및 보호에 관한 법률 시행령상의 정의규정
제2조(정의) ② 법 제2조제2호에서 "대통령령으로 정하는 정보"란 제1항에 따른 신용정보 중 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 정보로서 성명·주민등록번호 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 포함한다)를 말한다.

외국법령의 경우에도 구체적인 표현에 있어서는 조금씩 차이가 있지만 '개인정보'를 정의함에 있어 '식별가능성' 개념을 중심에 두고 있다는 점에서는 우리와 근본적인 차이가 있지는 않은 것으로 보인다. 이는 1980년 정립된 OECD 8원칙에 기초하여 1995년 등장한 EU 지침(EU Directive 95/46/EC)상의 개인정보 정의규정이 전 세계 개인정보 보호법제에 널리 수용되어 왔기 때문인 것으로 추정된다.[12]

위 EU 지침은 개인정보를 '식별된 또는 식별 가능한 자연인과 관련한 일체의 정보'라고 하면서 식별 가능한 자연인이라 함은 '직접 또는 간접적으로, 특히 이름, 식별번호를 참조하거나 해당인의 신체적, 심리적, 정신적, 경제적, 문화적 또는 사회적 정체성에 관한 하나 이상의 구체적인 특성을 참조함으로써 식별될 수 있는 자'를 의미한다고 규정하였다(제2.a항). 현재 이 정의는 2016년 선포된 EU (General Data Protection Regulation, EU Regulation 2016/679, 이하 "GDPR")에서도 거의 그대로 유지되고 있다(제4.a항).[13]

<표 2-4> 각국 법령상의 개인정보에 대한 정의

EU	개인정보는 식별된 또는 식별 가능한 자연인('개

12) 고학수·최경진, "개인정보의 비식별화 처리가 개인정보 보호에 미치는 영향에 관한 연구", 개인정보보호위원회(2015. 4).

13) EU GDPR 제4조 제a항에서는 개인정보를 정의함에 있어 본문에 인용된 기존 EU Directive에 대비하여 볼 때 위치정보, 온라인 식별자, 유전적 특성 정도의 개념요소를 추가하였다.
한편 EU GDPR은 전문 제26조에서 '식별가능성'에 대해 아래와 같이, 특정개인의 식별 등 처리자 또는 제3자 모두가 개인을 직접 또는 간접적으로 확인하기 위해 사용할 것으로 '합리적으로 예상되는 모든 수단'을 고려해야 한다고 하면서, 합리적으로 예상되는 수단인지 여부는 식별을 위해 소요되는 비용과 시간 등 객관적인 요소를 기준으로 하고, 이 때 처리 당시 사용 가능한 기술 및 기술적 발전을 모두 고려하여야 한다고 하고 있다.

GDPR 제4.a조[14]	인정보주체')과 관련한 일체의 정보를 가리킨다. 식별가능한 자연인은 직접 또는 간접적으로, 특히 이름, 식별번호, 위치정보, 온라인 식별자를 참조하거나 해당인의 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특이한 하나 이상의 요인을 참조함으로써 식별될 수 있는 자를 가리킨다.
영국 Data Protection Act 1998 제4조 제1항[15]	개인정보는 (a) 그 정보를 통해 (b) 그 정보 및 정보처리자의 소유하에 있거나 소유하에 있을 가능성이 높으면서 해당 자연인에 대한 견해 및 정보처리자 또는 어느 사람의 그 자연인에 대한 의도를 포함하고 있는 정보를 통해 식별될 수 있는 자연인에 관한 정보를 의미한다.
미국 Consumer Privacy Act 제4.7조[16]	개인정보란 특정 소비자 또는 장치에 대해 직·간접적으로 관련되어 있거나 연결되어 있거나 합리적 방법으로 연결될 수 있거나 아래를 포함하며 이에 한정되지 아니한다. (후략)
미국 Child Online Privacy Protection Act 제312.2조[17]	'개인정보'란 개인에 관해 개별적으로 식별 가능한 정보로써 온라인으로 수집된 것을 의미하며 이하를 포함한다. (후략)
독일 Bundesdatenschutzgesetz (BDSG) 제46조 제1호[18]	'개인정보'는 식별된 또는 식별 가능한 자연인('개인정보주체')과 관련한 일체의 정보를 가리킨다. 식별될 수 있는 자연인이란 이름, 식별번호, 위치정보, 온라인 식별자를 참조하거나 해당인의 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특이한 하나 이상의 요인을 참조함으로써 식별될 수 있는 자를 가리킨다.
일본 개인정보보호법 제2조 제1항	본법에 있어서 개인정보라 함은, 생존하는 개인에 관한 정보로서, 다음 각 호의 어느 하나에 해당하는 것을 가리킨다. 당해 정보에 포함되어 있는 성명, 생년월일 및 그 밖의 기술 등[문서, 도화 혹은 전자적 기록에 기재 혹은 기록되거나 또는 음성, 동작 및 그 밖의 방법을 사용하여 표시된 일체의 사항(개인식별부호를 제외함)]에 의해 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조하여 조합할 수 있고,

	그로써 특정의 개인을 식별할 수 있도록 되어 있는 것을 포함한다) 개인식별부호가 포함된 것
호주 The Privacy and Personal Information Protection Act 1998 제4.(1)조[19]	본 법에서 개인정보란 그로 인해 확정되었거나 합리적으로 확정될 수 있는 개인에 관한 정보 또는 견해를 의미한다. (데이터베이스 중 일부를 구성하는 정보를 포함하며, 물리적 실체를 구성하고 있는지 여부는 불문함)
캐나다 Digital Privacy Act 제2.1조[20]	개인정보는 식별 가능한 개인에 관한 정보이다.

14) personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

15) 현재 유효한 영국의 개인정보에 관한 법률은 Data Protection Act 2018로, 1998년법은 GDPR의 출범에 맞추어 개정되었다. (현행법은 개인정보의 개념 정의 부분에서 GDPR을 인용하고 있음) 위 Data Protection Act 1998은 이미 구법이 되었으나 개념 정의 방식을 참조하기 위하여 인용하였다.
"personal data" means data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

16) "Personal Information" means information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, including, but not limited to; (후략)"

17) "Personal information" means individually identifiable information about an individual collected online, including:

18) "personenbezogene Daten" alle Informationen, die sich auf eine

나. 개인정보 개념의 추상성으로 인한 개념 범위의 무한한 확장

추상적이고 모호한 법개념이 왜 문제가 되는지는 별도의 논의가 필요하지 않을 정도로 명확하다. 법률은 국민의 신뢰를 보호하고 법적 안정성을 확보하기 위하여 되도록 명확한 용어로 규정되어야 한다는 명확성의 원칙에 대한 헌법재판소의 풀이를 인용하자면, 규범의 의미내용으로부터 무엇이 금지되는 행위이고 무엇이 허용되는 행위인지를 수범자가 알 수 없다면 법적 안정성과 예측가능성은 확보될 수 없게 될 것이고, 또한 법집행 당국에 의한 자의적 집행을 가능하게 할 것이기 때문이다.[21]

국내법령에 개인정보 개념이 처음 정의된 1994년 이래로, 그간 관련 법률상 의개인정보의 정의는 실질적으로 변경된 부분이 없다고 보아도 무방하다. 현행 정보통신망법은 1994년 제정된 공공기관의개인정보보호에관한법률의 개인정보 개념에 부호, 문자, 음성, 음향 및 영상 등이라는 정보의 형태를 예시로 추가하고 식별이라는 한자어를 알아본다는 우리말로 바꾼 정도이다. 정보통신망법 제2조 정의규정상의 개인정보 개념은 다음과 같다.

---

identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann

19) "In this Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion."

20) Personal information means information about an identifiable individual.

21) 헌법재판소 1998. 4. 30. 선고 95 헌가16 결정

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

6. "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.

정보통신망법은 제4장에서 개인정보 보호 관련하여 정보통신서비스 제공자에게 부과되는 의무나 이용자의 권리 등을 규정하고 있다. 모든 권리의무에 관한 규정이 그 대상을 개인정보로 규정하고 있으나, 별도로 개별 의무 이행의 대상이 되는 정보의 범위를 직접적으로 구체화하는 조문은 없다. 앞서 표 2-2로 소개한 것과 같이, 개인정보가 처리되는 배경 또는 부대되는 사정에 비추어 동의의 범위 외로 처리할 수 있다던지 또는 동의 없이 처리할 수 있는 예외적인 상황을 허용해두고 있을 뿐이다. 결국 법문상으로만 볼 경우, 개인정보의 개념 범위가 곧 정보통신망법상 개인정보 관련 규제의 수범자 범위 그리고 부과되는 의무 범위를 사실상 결정하는 핵심적인 기준으로 기능하고 있다. 이러한 사실은, 개인정보 관련 법령 위반이 문제된 각종 분쟁에서, 많은 경우 핵심적인 쟁점이 문제된 정보가 개인정보에 해당하는지의 문제로 귀결된다는 점에 비추어서도 알 수 있다.

이와 관련하여 더욱 문제되는 점은 개인을 식별해낼 수 있는 정보의 범위가 나날이 넓어지고 있다는 사실이다. 데이터 수집 및 분석 기술은 계속하여 발전하고 있으며, 각종 정보통신서비스의 보편화 및 스마트폰 IoT 서비스를 통한 초연결 사회가 도래하면서 서비스 제공 사업자에게는 점점 더 많은 정보가 축적되고 있다. 서비스 사업자는 대부분 이용자의 기본적인 신상 정보를 파악하고 있으므로, 이용자가 서비스를 이용하는 과정에서 쌓이는 모든 정보 및 기록이 신상 정보와의 결합 가능성이 인정되어 이론상 개인정보에 해당할 수 있게 되는 것이다. 추상적 식별가능성만을 기준으로 개인정보에 해당하는지 여부를 판단할 경우, 사실상 개인정보에 해당하지 않는 정보가 존재하지 않는 실정에

이르렀다. 정보통신정책연구원에서도 Endpoint에서 생성되는 정보 비중이 높은 작금의 기술 환경과 고도의 데이터 분석 기술이 결합하면 식별정보를 전혀 이용하지 않았더라도 비자발적으로 식별가능한 상태가 될 가능성을 간과할 수 없다는 연구 결과를 내놓기도 하였다.[22]

이처럼 정보통신서비스 제공 사업자들이 보유하고 있는 개인에 관한 정보들은 스펙트럼이 매우 넓다. 개인정보에 해당한다는 점에 대해 반대하는 의견을 찾기 어려운 성명, 전화번호 등으로부터 시작하여 반대쪽 끝단에는 자신에 관한 정보는 아무것도 입력하지 않은 상태로 단순히 검색 사이트에 입력한 몇 가지 단어들마저도 모두 개인정보에 해당한다고 해석할 가능성이 존재한다.

다. 법 규정을 통한 개념 범위 획정의 한계

그럼에도 규제의 적용 단위는 앞서 짚어본 것처럼 개인정보라는 추상적인 요건으로 단일화되어 있기 때문에 정보통신망법을 제공받는 사업자의 관점에서는 법이 요구하는 의무 범위가 어디까지인지 알기 어렵다. 선행 연구[23]에 따르면 일반 국민과 공공기관 및 각 기업에서 실제 개인정보 처리 업무를 담당하는 실무자 각 집단을 대상으로 개인정보의 범위에 대한 인식조사를 실시한 결과, 일반 국민은 물론이고 실제 개인정보 관련 업무 수행 중인 실무자들 조차 어떤 경우에 다른 정보와 '쉽게' 결합할 수 있다고 볼 것인지 및 어느 정도가 되어야 특정 개인을 '알아볼(식별할) 수 있는 수준'에 이르렀다고 볼 것인지에 대해서 전혀 통일되지 않은 기준을 가지고 있음이 확인된바 있다. 특히 실무자

---

22) 개인정보 개념의 모호성을 지적하며 "Endpoint에서 생성되는 정보 비중이 높은 작금의 기술 환경과 고도의 데이터 분석 기술이 결합하면 식별정보를 전혀 이용하지 않았더라도 비자발적인 식별 가능성을 간과할 수 없다"고 지적한 선행 연구에 대해서는 조성은, "개인정보보호 법제 하에서의 정보 활용성 향상 전략", KISDI Premium Report 제17권 제12호(2017)를 참조.

23) 인하대학교 산학협력단(법학연구소), "개인정보의 범위에 관한 연구", 개인정보보호위원회(2014).

들이 항공 마일리지 카드번호, 회사 연락처 등 구체적인 정보 유형들에 대해 개인정보성을 판단하는 기준이 서로 상이하다는 점도 확인되었다.

이와 같은 상황에서는 개별 사업자가 스스로 법상의 의무를 모두 이행하고 있는 것인지 판단이 어렵고, 특정 시점에서 나름의 기준으로 현실적인 범위를 정하여 의무를 이행하면서도 특별히 법위반의 제재를 받고 있지 않다고 하더라도, 향후에도 그와 같은 상태가 유지될 것이라고 기대하기 어렵다. 특히 기업에 의한 개인정보 활용에 대해 늘 우려의 시선과 문제 제기가 쏟아지고 있다는 점에서 더욱 그렇다. 앞서 언급한 명확성의 원칙의 존재 이유가 여기서 드러난다. 규범의 의미내용으로부터 무엇이 금지되고 허용되는 행위인지를 수범자가 알 수 없는 상황이 도래하는 것이다. 그 결과 정보 활용에 있어서 매 구체적인 사안마다 법원의 최종 판단이 내려지기 전까지는 행위의 적법성에 대한 의심을 떨칠 수 없고, 정보의 이용이 위축될 수밖에 없다.

그러나 현행 정보통신망법이나 개인정보 보호법이 명확성의 원칙을 위배한 위헌의 소지가 있다는 것은 아니다. 명확성의 원칙이 언제나 최상의 명확성을 요구한다고는 볼 수 없을 뿐 아니라,[24] 통상적으로 법률규정은 일반성, 추상성을 가지는 것으로서 입법기술상 어느 정도의 보편적 내지 일반적 개념의 용어사용이 부득이하다[25]는 것을 인정하는 것이야말로 명확성의 원칙의 전제이며 설득력의 근가 된다. 이 때 일반적 개념의 용어사용이 어느 정도까지 허용되는지에 대해 헌법재판소가 제시한 기준은 “당해 법률조항의 입법취지와 전체적 체계 및 내용 등에 비추어 법관의 법 보충작용으로서의 해석을 통하여 그 의미가 분명해질 수 있는지 여부”이며,[26] 대법원 역시 유사한 취지로 설시하고 있다.[27]

---

24) 헌법재판소 2005. 6. 30. 선고 2002헌바83결정 등
25) 헌법재판소 2016. 7. 28. 선고 2014헌바421 결정
26) 상동
27) 대법원 2010. 5. 27. 선고 2009두1983 판결
“기본권제한입법이라 하더라도 규율대상이 지극히 다양하거나 수시로 변화하는 성질의 것이어서 입법기술상 일의적으로 규정할 수 없는 경우에는 명

결국 개인정보 관련 규제가 합리성을 확보하고 규제 실질화를 이루기 위해 필요한 것은 법률조항의 입법취지와 전체적 체계, 내용 등에 비추어 의미를 분명케 하는 작업이다. 그러나 일부 분쟁 상황에서 문제된 정보 항목에 대해 산발적으로 개인정보성을 판단하여 온 판결들을 제외하고, 현 시점에서 법령상의 개별 의무에 대응하여 적합한 의무 이행의 범위 등을 해석상 도출하려는 시도는 적극적으로 이루어져 오지 않은 것으로 보인다.[28)]

3. 개인정보 개념 및 규제 적용범위에 대한 구체화 시도

현행 법령상 개인정보의 개념이 추상적이고 모호하게 규정되어 있어 개선이 필요하다는 점에 대하여는 이미 지속적으로 문제가 제기되어 왔다. 학계와 기업 및 언론에서 규제의 불확실성 및 빅데이터 등 4차 산업 발전의 저해를 초래할 가능성 등에 대해 환기한 끝에, 정부에서도 유사한 문제 의식을 갖게 된 것으로 보인다. 대표적으로 정부는 2016. 5.경 국무조정실 차원에서 '개인정보 개념 명확화'를 신산업-현장 제기 규제혁파 과제로 선정하기도 했다.[29)]

확성의 요건이 완화되어야 할 것이다. 또 당해 규정이 명확한지 여부는 그 규정의 문언만으로 판단할 것이 아니라 관련 조항을 유기적·체계적으로 종합하여 판단하여야 할 것이다."

28) 개인정보자기결정권과 표현의 자유 및 영업의 자유 등 다른 헌법적 가치의 충돌에 있어서 헌법적 균형 유지의 필요성을 강조하고, 개인정보별 보호 정도의 차등화가 가능한지에 대한 검토가 필요하다고 지적한 연구결과로는 황성기, "개인정보 보호와 다른 헌법적 가치의 조화", 경제규제와 법 제5권 제2호(2012) 참조.
위 논문에서는 예컨대 개인정보를 보호가치 내지 그 성격에 따라 '민감정보'와 '비민감정보', '고유식별정보'와 '비고유식별정보', '성향중립 개인정보'와 '성향기반 개인정보', '개인에 관한 정보'와 '협의의 개인정보', '공적 영역의 개인정보'와 '사적 영역의 개인정보' 등 다양한 방식으로 분류하여 그 유형별로 보호 정도를 달리하는 방식의 접근을 제안하고 있다.

29) 해당 과제의 현황 및 문제점으로는 다음과 같은 내용이 기재되어 있다.

한편 국회 역시 개인정보 개념의 불명확성 문제를 입법적으로 해소하고자 개인정보 보호법 및 정보통신망법상 개인정보 정의 규정을 명확히 하는 개정안 등의 시도를 지속하여 왔고, 근래에는 정의규정의 개정을 포함하는 개인정보 보호법 개정안이 다수 발의되기도 했다. 2018. 11. 15. 인재근의원 등 14인이 공동 발의한 개인정보 보호법 일부개정법률안에서는 개인정보의 개념 체계를 개인정보, 가명정보, 익명정보로 구분하고, 개인정보와 가명정보까지를 개인정보 보호법상 '개인정보'로 정하면서도, 가명정보는 통계작성, 연구, 공익적 기록보존의 목적으로 처리할 수 있도록 예외 규정을 마련하였다.[30]

이와 같이 개인정보의 정의로부터 파생되는 문제점에 대해, 정의 규정의 직접적인 개선 및 수정을 해결방법으로 제시하는 식의 접근은 이미 충분히 이루어지고 있는 것으로 보인다. 개인정보의 개념 정의를 보다 구체화함으로써 문제의 소지를 줄이는 것 역시 필요하겠으나, 전세계적으로도 개인정보의 범위가 유사하게 정의되어 있는 점에 비추어 볼 때 일반개념 자체를 수정하면서도 합리성을 유지하기는 쉽지 않을 것으로 보이며, 이를 통하여 현재 필요로 하는 구체성을 충분히 획득하기도 어려울 것으로 생각된다.

개인정보 개념의 명확화에 관한 상기 규제 혁파 과제를 행정안전부(당시 행정자치부)와 방송통신위원회가 주도적으로 추진한 결과물을 보더라도, 개선 내용으로 관련부처와 합동으로 개인정보 개념을 구체화하는 방안 등을 위해 개인정보 관련부처 통합 법 해설서를 마련하였다는 점이 제시되어 있다. 개념을 직접 구체화하기보다는 법령 해설을 통해 가능한 범위에서 기준을 명시하는 방안을 택한 것이다.

·현재 개인정보의 개념이 모호하여 '개인정보보호법' 적용대상 확대 우려

·개인정보의 추상적 결합 및 무한 확장 가능성 등을 통해 관련 산업의 발전을 저해

·현행 개인정보 규정은 다른 정보와 쉽게 결합하여 알아볼 수 있는 것'을 개인정보에 포함시키는 등 추상적 정의로 인해 규제 불확실성 증대

30) 인재근 의원 대표발의, "개인정보 보호법 일부개정법률안", 2016621, (2018. 11. 15.) [계류중], 5(제2조 제1호).

이와 같이 그간 정부 차원에서는 개인정보 보호 법령 및 관련 규제를 원활하게 현실에 적용하고 집행하기 위한 방편으로, 각종 가이드라인이나 지침서 등을 통해 정부가 제시하는 기준을 공표하여 왔다.

<표 2-5> 개인정보 관련 주요 가이드라인 목록

발행시기	명칭	발행기관
2018. 11.	온라인 개인정보 처리 가이드라인 개정안 (2014. 11.안에 대한 개정안)	방송통신위원회 한국인터넷진흥원
2018.6.	개인정보 처리 위수탁 안내서	행정안전부
2017. 12.	바이오정보 보호 가이드라인	방송통신위원회 한국인터넷진흥원
2017. 12.	개인정보의 기술적•관리적 보호조치 기준 해설서	방송통신위원회 한국인터넷진흥원
2017. 2.	온라인 맞춤형 광고 개인정보보호 가이드라인	방송통신위원회 한국인터넷진흥원
2017. 1.	개인정보의 안전성 확보조치 기준(개정, 2016.9.1. 행정자치부 고시 제2016-35호) 해설서	행정안전부 한국인터넷진흥원
2016. 12.	개인정보의 안전성 확보조치 기준 해설서	행정안전부 한국인터넷진흥원
2016. 12.	금융분야 개인정보보호 가이드라인	금융위원회 금융감독원 행정안전부
2016. 12.	개인정보보호 법령 및 지침•고시 해설서	행정안전부
2016. 11.	개인정보 수집 최소화 가이드라인	행정안전부 한국인터넷진흥원
2016. 6.	개인정보 비식별 조치 가이드라인	국무조정실 외 5개 부처
2015. 2.	의료분야 개인정보보호 가이드라인	보건복지부 행정안전부
2015. 2.	개정 정보통신망법 중 개인정보보호 규정 안내서	방송통신위원회
2014. 12.	빅데이터 개인정보 보호 가이드라인	방송통신위원회
2014. 11.	온라인 개인정보 취급 가이드라인	방송통신위원회

2012. 8.	개정 정보통신망법 개인정보보호 신규 제도 안내서	방송통신위원회 한국인터넷진흥원
2011. 1.	정보통신서비스 제공자를 위한 개인정보보호 가이드	방송통신위원회 한국인터넷진흥원

그러나 위와 같은 가이드라인 자료들은 정부의 법 해석 기준 및 지침을 공개한 것으로써 예측가능성이나 법적 안정성에 일조하는 측면은 분명하나, 여전히 개인정보의 넓은 의미 범위를 기초로 하고 있기 때문에 탄력적인 해석의 여지 측면에서 실마리를 얻기는 어렵다. 특히 개인정보 비식별 조치 가이드라인 이나 온라인 맞춤형 광고 개인정보보호 가이드라인과 같이 개인정보의 활용을 촉진시키고자 하는 목적으로 제시된 가이드라인들의 경우, 그 내용이 불분명하다거나 심지어는 법의 취지에 위배된다는 지적마저 받고 있는 상황이다.

따라서 본 연구서에서는 규제 적용범위와 관련하여 기존에 이루어진 시도와는 다른 방향으로 접근하고자 한다. 개인정보의 보호와 이용이 서로 충돌할 수밖에 없는 상황에서, 개인정보 처리과정에서 법령에 의해 부과되는 의무별로 개인정보의 범위를 서로 달리 해석하여 규제 합리화를 꾀할 수 있도록 일응의 객관적인 기준을 제시하고자 한다. 특히 앞서 지적한 것과 같이 개인정보에 관한 권리가 적극적인 통제권으로 이해되고 있는 것과 관련하여, 이용자가 행사할 수 있는 통제권의 내용이나 범위에 대하여 보다 적극적으로 검토하여 볼 필요가 있다. 아래에서는 본격적인 논의에 앞서, 동일하게 사용된 법률용어를 서로 달리 해석할 수 있는 논리적인 근거 및 타 법령상의 사례에 대해 먼저 살펴보도록 하겠다.

제 2 절 차등적인 법해석의 가능성

이상에서 살펴본 바와 같이 정보통신망법은 개인정보의 개념을 추상적인 문구로 정의하고 있으며, 이로 인한 개인정보 개념의 모호성은 동법의 수범자로

하여금 그가 준수하여야 하는 법령상 의무의 내용과 범위를 예측하기 어렵게 한다는 점에서 법적 안정성을 저해하는 요인으로 작용하고 있다. 그러나 이와 같은 법령 단계에서의 불명확함은 해석을 통하여 보완될 수 있다. 정의 규정에서 제시하는 식별가능성, 결합의 용이성 등의 개념 요소는 적절한 해석을 통해 법령이 합목적적으로 운용될 수 있는 기초가 된다.

아래에서는 법률 해석의 방법에 관한 이론을 간략히 정리한 후, 실제로 동일한 법적 용어가 구체적인 규정 또는 사안에 따라 달리 해석되는 사례들을 살펴보고, 정보통신망법상 "개인정보"의 개념 또한 그와 같이 입체적으로 해석되어야 할 필요가 있음을 논하기로 한다.

1. 불확정개념이 사용된 경우의 법해석 방법

전통적인 법학방법론에서는 법해석의 방법론을 문리적 해석, 논리적 해석, 역사적 해석, 목적론적 해석의 4가지로 구분하여 왔다.[31]

<표 2-6> 법리 해석의 유형

문리적 해석	법률문언의 일반적인 의미를 평가하여 개별적인 사항을 포섭시키는 법해석 방법.[32]
논리적 해석	법규의 논리적 맥락 및 체계적인 관계에 관한 이해를 바탕으로 법을 해석하는 방법[33]
역사적 해석	입법자가 법률을 제정할 당시 의도했던 계획에 맞게 법을 해석하는 방법(주관적 해석이라고도 불림)[34]
목적론적 해석	법질서에서 객관적으로 요구되는 "이성적인 목적"에 따라 법규의 의미를 파악하는 방법(객관적 해석이라고도 불림)[35]

31) 심헌섭, "법철학적 법학방법론 - 법철학과 합리적 법학방법", 서울대학교 법학 제24권 제1호(2003), 5.

32) 권순희, "전통적 법해석방법과 법률해석의 한계", 가톨릭대학교 법학연구소 법학연구(2009), 138.

법원 역시 이와 같은 법해석 이론을 재판 규범으로 받아들여왔다. 한국수자원공사의 사장이 변호사법상 취급사건에 대한 청탁 내지 알선을 명목으로 하는 이익 수취 등의 금지가 적용되는 “법령에 의하여 공무원으로 보는 자”에 해당하는지가 쟁점이 된 사건에서 대법원은 위와 같은 해석의 유형을 직접 거론하면서, 특히 목적론적 해석에 대하여 법질서 전체의 이념, 법규의 기능, 입법 연혁, 입법 취지 및 목적, 보호법익과 보호의 목적, 행위의 형태 등 여러 요소를 종합적으로 고려하여야 한다고 판시한바 있다.[36] 또한 구 임대주택법상의 ‘임차인’의 의미에 대해 해석한 판결에서는, 이와 같은 법 해석 시에는 법의 표준적 의미를 밝혀 객관적 타당성이 있도록 하여야 하고, 가급적 모든 사람이 수긍할 수 있는 일관성을 유지함으로써 법적 안정성이 손상되지 않도록 하면서도 구체적 타당성을 가질 수 있도록 하여야 한다는 요건을 제시하기도 했다.[37]

위와 같은 4가지 법해석 방법은 상호보완적인 성격을 가지고 있는 것으로서, 그 중 어느 하나의 방법론이 다른 방법론에 비해 우월하다거나 특별한 중요성을 가지고 있다고는 말하기는 어렵다. 그러나 목적론적 법해석은 법질서에서

---

33) 권순희, 위 논문, 142.
34) 권순희, 위 논문, 146.
35) 권순희, 위 논문, 149.
36) 대법원 2006. 11. 16. 선고 2006도4549 판결
“형벌법규의 해석 역시 그 규범적 의미를 명확히 하여 이를 구체적 사실에 적용할 수 있도록 하는 작업으로서, 죄형법정주의의 요청상 위와 같은 제한이 있기는 하나, 다른 법률과 마찬가지로 우선 법문상 어구나 문장의 가능한 언어적 의미내용을 명확하게 하고(문리해석), 동시에 다른 법률과의 관련성 등을 고려하여 논리적 정합성을 갖도록 해석하여야 하는 것이며(논리해석), 형벌법규의 문언이나 논리에 따르는 것만으로는 그 규정의 법규범으로서 의미를 충분히 파악할 수 없는 경우에는 법질서 전체의 이념, 그 형벌법규의 기능, 입법 연혁, 입법 취지 및 목적, 그 형벌법규의 보호법익과 보호의 목적, 행위의 형태 등 여러 요소를 종합적으로 고려하여, 형벌법규의 통상적인 의미범위 내에서 그 의미를 구체화할 수 있는 것이다(목적론적 해석).”
37) 대법원 2009. 4. 23. 선고 2006다81035 판결

객관적으로 요구되는 이성적인 목적에 따라서 법규의 의미를 찾는 해석방법론으로서, 법률의 문언과 논리적 체계를 넘어서는 체계초월적 해석 방법론으로 평가되며,[38] 소위 법실증주의의 한계를 극복하고 사회적인 현실을 고려한 합목적적 문제해결을 도모하기 위한 핵심적인 도구로 기능한다는 점에서 독자적인 중요성을 가진다.[39]

문리해석에 따른 법해석 결과가 불합리한 경우 목적론적 해석은 특히 중요해진다. 다음에서 소개하는 판례 내지는 학설들은 명시적으로 목적론적 해석이라는 용어를 사용하고 있지는 않으나, 문리해석에 따른다면 같은 의미로 해석되어야 할 법률 문언을 그 적용 사안 유형별 규율 목적에 따라 다른 의미로 해석하고 있다는 측면에서 목적론적 법해석의 일례로 평할 수 있다..

2. 동일한 법개념이 규정에 따라 차등해석되는 사례

가. 형법상의 폭행 개념

형법은 소요죄, 공무집행방해죄, 폭행죄, 강도죄 등 "폭행"을 구성요건으로 하는 다수의 범죄에 관하여 규정하고 있으나, 각각의 폭행이 무엇을 의미하는가에 대하여는 명확한 정의 규정을 두고 있지 아니하여 그 의미는 해석에 맡겨져 있다. 폭행을 구성요건으로 하는 범죄의 유형이 매우 다양하기 때문에, 각각의 범죄를 구성하는 폭행이라는 행위를 동일하게 해석할 경우 합리적인 결론에 이르지 못할 우려가 있다. 이로 인하여 통설은 범죄의 유형에 따라 폭행의 의미를 달리 해석하여야 한다는 것이며,[40] 판례도 이를 받아들이고 있다.

---

38) 김학태, "법률해석의 한계 - 판례에서 나타난 법해석방법론에 대한 비판적 고찰", 외법논집 제22집(2006), 191.

39) 김학태, 위 논문, 201-202면.

40) 김성돈, 형법각론(제4판), 성균관대학교 출판부(2016), 80-81; 배종대, 형법각론(제8판), 홍문사(2013), 105; 이재상 외 2인, 형법각론(제10판), 박영사(2016), 60-61. 한편 이에 비판적인 견해로는 오영근, 형법각론(제3판), 박영사(2014),

<표 2-7> 형법상 '폭행' 개념에 대한 해석례

최광의의 폭행	• 소요죄(제115조), 다중불해산죄(제116조)의 구성요건 • 유형력이 불법하게 행사되는 모든 경우를 포함하는 것으로 넓게 해석됨 • 내란죄(제87조)의 구성요건에는 폭행과 유사한 "폭동"이라는 문구가 사용되었는데, 이는 유형력 행사의 대상에 사람뿐만 아니라 물건까지 포함시킨 개념으로 해석됨
광의의 폭행	• 공무집행방해죄(제136조 제1항), 직무강요죄(제136조 제2항), 특수도주죄(제146조), 공무원의 폭행·가혹행위죄(제125조), 강요죄(제324조 제1항)의 구성요건 • 사람에 대한 유형력의 행사를 의미하나 반드시 사람의 신체에 대하여 유형력이 가해짐을 요하지 않는 것으로 넓게 해석됨 • 물체에 대하여 가해진 유형력일지라도 그것이 사람의 신체에 물리적으로 감응을 일으킬 수 있는 것이면 족하다고 봄
협의의 폭행	• 폭행죄(제260조), 강제추행죄(제298조)의 구성요건 • 유형력이 사람의 신체에 대하여 가해지는 경우에 한정되는 것으로 해석되어 의미 범위가 상대적으로 좁음.
최협의의 폭행	• 강도죄(제333조), 준강도죄(제335조) 등의 구성요건 • 사람에 대한 유형력의 행사로서 그 사람의 반항을 억압하기에 충분할 정도로 강력한 유형력의 행사일 것을 요하는 것으로 해석되어 의미 범위가 가장 좁음.

이와 같은 차등적인 해석은 각 범죄의 특성에 비추어 볼 때 타당성이 인정된다. 예를 들어, 소요죄나 다중불해산죄의 경우 다중이 집합하여 공공의 안전을 해하는 행위를 저지르는 것을 방지하기 위하여 처벌규정을 둔 것이므로, 해당 범죄행위로서 형벌을 가하여야 할지 여부를 판단함에 있어서는 유형력의 행사 태양을 개별 행위자가 특정 피해자에게 유형력을 행사하여 개인적 법익을 침해하는 범죄와는 달리, 소위 사회적 법익의 침해가 발생하였다고 볼 수 있는지 여부를 중요하게 심사하여야 한다. 따라서 개별 행위자가 행사한 유형력의 태양을 반드시 타인의 신체 등으로 한정할 필요성이 적으므로 위와 같이 광의의

64-66.

폭행 개념을 적용하는 것이라고 볼 수 있다. 반면 폭행죄나 강도죄 등의 제추행죄의 경우 폭행행위로서 타인의 신체적 법익을 침해한 것 자체가 비난가능성의 핵심이 되는 범죄이므로, 폭행행위의 범위를 적절히 한정해야 할 필요성이 높다. 따라서 소요죄나 다중불해산죄와는 달리 폭행의 개념을 사람의 신체에 직간접적으로 유형력을 가하는 행위로 좁게 해석할 필요가 있을 것이다.

나아가 강도죄의 경우, 공갈죄와 비교하여 보았을 때 폭행을 매개행위로 하여 타인으로부터 재물이나 재산상의 이익을 빼앗는다는 점에서 두 범죄는 서로 유사하다. 그러나 법정형을 기준으로 비교해 보면 공갈죄는 10년 이하의 징역 또는 2천만 원 이하의 벌금으로 규정되어 있는 것에 비해, 강도죄는 3년 이상의 유기징역으로 규정되어 있어 훨씬 중하게 처벌된다. 이에 비추어 볼 때 강도죄의 비난가능성은 공갈죄보다 중하므로, 행위 수단이 더욱 한정되어 사람에 대한 유형력의 행사로서 그 반항을 억압할 수 있는 정도에 이르러야 한다고 해석되고 있다.

나. 형법상의 협박 개념

폭행의 사례와 유사하게 형법상 협박을 구성요건으로 하는 범죄도 다수 규정되어 있으며, 각각의 범죄유형별로 협박의 의미도 아래 표와 같이 차등적으로 해석되고 있다.[41] [42]역시 각 범죄의 성격 내지는 보호법익에 비추어 달리 해석되는 것으로 이해되는데, 예컨대 공무집행방해죄의 경우 소위 추상적 위험범으로서, 공무집행이 현실적으로 방해되었을 것을 그 구성요건으로 하지 않으므로,[43] 행위수단인 협박에 대한 해석에서도 '상대방에게 현실적으로 공포심을

41) 김성돈, 앞의 책, 123-124; 배종대, 앞의 책, 186-187; 이재상 외 2인, 앞의 책, 118. 비판하는 견해로는 오영근, 앞의 책, 109-110.

42) 공무집행방해죄에 관하여 대법원 2006. 1. 13. 선고 2005도4799 판결, 협박죄에 관하여 대법원 1991. 5. 10. 선고 90도2102 판결, 강간죄에 관하여 2007. 1. 25. 선고 2006도5979 판결 등.

43) 대법원 2018. 3. 29. 선고, 2017도21537 판결 참조.

느끼게 할 것'이 요구되지 않는다. 반면 협박죄나 공갈죄의 경우 협박 그 자체가 비난가능성의 핵심이므로, 상대방에게 현실적으로 공포심을 느끼게 하였을 것을 요구함으로써 처벌의 범위를 제한하고 있다.

<표 2-8> 형법상 '협박' 개념에 대한 해석례

광의의 협박	• 외국원수협박죄(제107조), 외국사절협박죄(제108조), 공무집행방해죄(제136조 제1항), 직무강요죄(제136조 제2항), 특수도주죄(제146조)의 구성요건 • 사람에 대한 유형력의 행사를 의미하나 반드시 사람의 신체에 대하여 유형력이 가해짐을 요하지 않는 것으로 넓게 해석됨
협의의 협박	• 협박죄(제283조), 공갈죄(제350조), 강요죄(제324조)의 구성요건 • 객관적으로 상대방이 공포심을 느낄 수 있을 정도의 해악을 고지하는 것에 더하여, 상대방이 현실적으로 공포심을 느꼈을 경우에만 기수가 인정되는 것으로 해석되므로 그 의미 범위가 상대적으로 좁음
최협의의 협박	• 강간죄(제297조), 강도죄(제333조), 준강도죄(제335조) 등의 구성요건 • 상대방의 반항을 억압할 정도의 공포심을 불러일으키는 고도의 해악을 고지하는 경우로서 가장 좁게 해석됨.

다. 형법상의 허위 개념

형법상 "허위"라는 요건 역시 서로 다른 규정에서 다의적으로 해석되고 있는데, 대표적인 것이 위증죄와 무고죄의 사례이다. 법률에 의하여 선서한 증인이 허위의 진술을 한 때 성립하는 위증죄[44]에서 말하는 '허위의 진술'이란, 증인이 자기의 기억에 반하는 사실을 진술하는 것을 가리키며, 그 내용이 객관적 사실과 부합하는지 여부를 불문한다.[45] 반면 타인으로 하여금 형사처분 또

44) 형법 제152조 제1항
45) 대법원 1989. 1. 18. 선고 88도580 판결 참조.

는 징계처분을 받게 할 목적으로 공무소 또는 공무원에 대하여 허위의 사실을 신고한 때 성립하는 무고죄[46]에서의 허위 신고는 신고사실이 객관적 사실에 반한다는 것을 확정적이거나 미필적으로 인식하면서 신고하는 것을 의미하며, 허위라고 믿고 신고하였다 하더라도 객관적으로 진실한 사실에 부합할 경우 허위신고에 해당하지 않는다고 해석되고 있다.[47]

진술 내지 신고사실이 허위인지를 행위자를 기준으로 하여 주관적으로 판단할지 아니면 진실한 사실관계를 기준으로 하여 객관적으로 판단할지에 관하여 판례는 위증죄와 무고죄에 대해 정반대의 해석을 차용하고 있는데, 이 또한 각 처벌규정의 목적에 비추어 이해할 수 있다. 우선 양 범죄는 국가의 형사사법권 또는 징계권의 적정한 행사를 그 보호법익으로 한다는 점에서 공통된다. 그런데 허위사실의 신고는 수사관서 또는 감독관서로 하여금 수사 내지 조사를 개시하게 하는 단서가 될 뿐이지만, 허위의 증언은 특정 사안에 관한 최종적 판단 단계인 재판의 근거로 쓰인다는 점에서 그 진실성의 확보가 상대적으로 중요하다고 평가할 수 있다.[48] 따라서 무고죄는 침해범으로 보아 신고사실의 허위성을 판단함에 있어 그것이 객관적 진실에 부합하는 경우 처벌하지 않는 반면 위증죄는 이른바 추상적 위험범으로 보아 증인이 그 기억에 반하는 진술을 한 경우 그것이 객관적 진실에 부합하더라도 처벌을 면하지 못한다.

라. 민법상의 선의 개념

민법에서도 동일한 법문언을 서로 달리 해석하는 사례가 발견된다. 대표적인 예시로서 “선의”에 대한 해석이 있다. 일반적인 법률용어로서 선의란 자신의 행위가 법률관계의 발생, 소멸 및 그 효력에 영향을 미치는 사실을 모르는 일

---

46) 형법 제156조
47) 대법원 1982. 4. 27. 선고 81도2341 판결 참조.
48) 유사한 취지로 김대휘·김신 편집대표, 주석 형법(각칙 2)(제5판), 한국사법행정학회(2017), 73-75.

을 의미하며, 악의는 그 반대의 경우를 의미한다.

선의 개념은 특정한 사실관계에 관하여 선의인 자에 대하여 그러한 사실관계로 인한 법률효과를 부인할 수 있는 권능을 부여하는 규정에 널리 사용된다.[49] 해당 규정들을 적용함에 있어 선의 개념은 단일한 의미로 해석되지 않고 있는데, 주로 특정한 사실관계에 대해 선의인 자가 사실관계를 모른 데에 과실 또는 중과실이 있는 경우가 문제된다.

예를 들어 민법은 상대방과 통정한 허위의 의사표시는 무효라고 규정하고 있지만(제108조 제1항), 특정한 의사표시가 이러한 통정허위표시에 해당한다는 사실을 모른(선의의) 제3자는 그로 인한 의사표시의 무효를 부인할 수 있도록 되어 있다(제108조 제2항). 이 때 대법원 판례상 선의의 제3자는 통정허위표시를 모른 데 대하여 과실이 있는지 여부를 불문하고 보호받는다.[50]

법문상으로는 통정허위표시로 인한 의사표시의 무효를 "선의의 제3자에게 대항하지 못한다"라고만 규정되어 있고, 비록 과실로 알지 못했다고 하더라도 선의가 악의로 전환되는 것은 아니므로 위와 같은 결론은 일견 타당해보인다. 그러나 '선의의 제3자'가 항상 위와 같이 해석되는 것은 아니다.

일례로 채권양도의 경우를 들 수 있다. 민법은 채권의 양도가능성에 대해 성질상 양도가 불가능한 경우 외에는 일반적으로 양도 가능한 것으로 규정하면서(제449조 제1항), 채권자와 채무자 사이에 해당 채권을 양도하지 아니하기로 약정할 수 있도록 하고 있다(소위 `양도금지특약`, 제449조 제2항 본문). 만약 채

---

49) 몇 가지만 예를 들자면, 실종선고의 취소(제29조), 비진의표시/통정허위표시로 인한 의사표시의 무효(제107, 108조), 착오/사기/강박으로 인한 의사표시의 취소(제109, 110조), 소위 표현대리(제125, 126, 129조), 시효취득(제245, 246조), 선의취득(제249조), 채권양도금지특약에 반하는 채권양도(제449조 제2항), 채권의 준점유자에 대한 변제(제470조), 상계금지특약에 반하는 상계(제492조 제2항), 부당이득반환(제748조) 등이 있다.

50) 대법원 2004. 5. 28. 선고 2003다70041 판결 참조. 통설도 같은 견지에 있다: 김용담 편집대표, 주석 민법 총칙(3)(제4판), 한국사법행정학회(2010), 627.

권자가 양도금지특약에 반하여 채권을 양도한 경우, 양도금지특약의 존재를 모르고(선의) 채권을 양수한 제3자는 채무자와의 관계에서 해당 양도금지특약의 존재를 부인할 수 있다(제449조 제2항 단서). 그러나 중대한 과실로 인하여 이와 같은 양도금지특약의 존재를 모른 자는 선의의 제3자로 보호받지 못한다.[51]

결국 양도금지특약에 반하여 채권을 양수한 자의 보호 범위에 관하여 민법이 규정한 `선의'라는 개념은 통정허위표시의 경우와는 달리 중과실로 사실(이 경우 양도금지특약)을 알지 못한 경우를 제외하는 것으로 의미가 축소해석되고 있음을 알 수 있다.

그 이유는 비교적 명확한데, 통정허위표시의 경우 허위표시의 당사자는 고의로 진실과 일치하지 아니하는 외관을 창출한 자들임에도, 제3자가 그러한 허위표시 사실을 알 수 있었다는 이유로 허위표시의 무효를 주장할 수 있게 하는 것은 부당하지만,[52] 채권양도금지특약은 법률상 정면으로 허용되는 것(제449조 제2항 본문)이므로 그와 같은 특약의 존재를 조금만 주의를 기울이면 알 수 있었음에도 이를 알지 못한 제3자는 통상의 경우와 같이 악의와 동일하게 다루어도 무방하다는 것이다.[53]

3. 소결

이상과 같이 동일한 법문이 목적에 따라 다른 의미로 해석 내지 정의되는 사례는 다른 실정법 분야에서도 확인된다. 나아가 도로교통법상의 '운전' 개념과 같이 필요에 따라 단일한 법률에서 같은 용어를 다의적으로 정의하는 사례도 발견된다.[54]

---

51) 대법원 1996. 6. 28. 선고 96다18281 판결 참조.

52) 윤진수, "허위표시와 제3자", 민사판례연구 제29권(2007), 593-595.

53) 김형배, 채권각론(제2판), 박영사(2001), 577; 김상용, 채권각론(제2판), 화산미디어(2014), 393 등.

54) 도로교통법상 "운전"의 의미를 "도로에서 차마를 그 본래의 사용방법에 따라 사용하는 것"으로 정의하면서, 음주운전(동법 제44조, 제148조의2) 또

개인정보 자기결정권은 현대에 이르러 생성된 권리로서, 장기간에 걸쳐 고찰된 전통적인 권리와 달리 아직까지 개념이 형성되는 과정에 있다. 이러한 점을 고려하면, 개인정보야말로 목적론적 해석, 차등적 해석을 통해 권리의 보호범위를 실질적으로 규명할 필요가 있으며, 그러한 해석에는 개인정보를 둘러싼 여러 가지 가치와 이익이 모두 고려되어야 할 것이다. 다음 항에서는 이와 같은 이론적인 기초에 따라, 차등해석이 실제로 어떻게 구현될 수 있을지와 관련하여, 개인정보를 유형별로 분류해보면서 차등해석의 기준을 제시하도록 하겠다.

는 뺑소니(제54조 제1항, 제148조, 제156조 제10호) 등을 금지 및 처벌하는 규정에서는 운전의 의미를 확대하여 도로가 아닌 곳에서의 차마의 사용까지 포함하고 있다(제2조 제26호).

> 도로교통법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
> (중략)
> 26. "운전"이란 도로(제44조·제45조·제54조제1항·제148조·제148조의2 및 제156조제10호의 경우에는 도로 외의 곳을 포함한다)에서 차마를 그 본래의 사용방법에 따라 사용하는 것(조종을 포함한다)을 말한다.

제 3 장 개인정보의 유형별 분류

제 1 절 서론

앞서 살펴본 것처럼 추상적인 개념 요소 및 정의로 인하여 지극히 넓은 개념 범위를 갖게 된 개인정보는, 그만큼 다양한 기준에 따라 분류되거나 또는 유형화될 수 있다. 정보의 내용에 따른 구분만을 보더라도, 개인정보보호위원회 또는 한국인터넷진흥원(이하 "KISA")는 개인정보의 개념에 대해 설명하면서 총 16가지 유형의 개인정보를 예시로 들고 있다.[55] 학계에서는 그 외에도 컴퓨터 처리 여부, 자동처리 여부, 식별의 난이도, 고유성 유무, 침해위험의 크기, 정보의 출처, 공개여부, 성격, 진술대상, 권리의 배타성 유무, 표현 전달 수단,[56] 관리주체 또는 정보주체 등의 여러 가지 분류기준을 활용하여 개인정보를 유형화하려고 시도하고 있는 것으로 보인다.

이와 같이 개인정보를 유형별로 분류하려는 시도는 학문적인 의미나 만족만을 위한 것이 아니다. 물론 모든 분류가 실질적으로도 각 유형간의 차별성을 드러냄으로써 규범의 해석이나 적용 측면에서 의미를 갖는 것은 아닐 것이다. 그러나 일정한 성상에 따라 개인정보를 분류해보는 과정에서 과연 어떠한 정보까지 개인정보로 취급해야 하는 것인지 검토하여 볼 계기가 계속하여 생겨나고, 객관적인 분류 기준이 누적하여 수립되는 과정에서 개인정보의 범위 획정에 기여할 수도 있다. 이러한 과정 속에서 개인정보의 넓은 개념 범위 속에 존재하는 특정한 정보에 대해, 타인이 취급 가능한 정보인지 또는 그에 대한 적

---

55) 개인정보보호위원회 및 KISA 홈페이지 참조
일반정보, 가족정보, 교육 및 훈련정보, 병역정보, 부동산정보, 소득정보, 기타 수익정보, 신용정보, 고용정보, 법적정보, 의료정보, 조직정보, 통신정보, 위치정보, 신체정보, 습관 및 취미정보

56) 이창범, 개인정보 보호법, 법문사(2012), 21 등

정한 취급 수준을 어떻게 설정하여야 할지 검토해봄으로써, 궁극적으로는 해당 정보가 보호 또는 이용의 대상 중 어느 쪽에 얼만큼 더 가까운 것인지에 대한 판단을 통해 개인정보 보호 관련 제도의 내용에도 영향을 미칠 수 있다.

현행법을 기준으로 살펴볼 때, 법령상 개인정보에 대한 명시적인 분류라고 볼 수 있는 것은 개인정보 보호법상의 개인정보, 민감정보 그리고 고유식별정보의 구분 정도가 유일하다.[57] 그 외에 2018. 11. 현재 발의되어 있는 개인정보 보호법 개정안[58]에는 식별성을 제거하는 조치 수준에 따른 분류가 추가되어 '가명정보', '익명처리를 한 정보'의 개념이 도입되어 있기도 하다. 이와 같은 분류 역시 개인정보의 보호 또는 활용의 수준을 대상마다 달리 정하기 위한 것이다.

규제 유형별 보호범위의 차등화를 목적으로 하는 본 연구서에서는, 학계에서 소개되는 다양한 분류 중 규제 유형별 차등 취급의 필요성이 떨어지는 내용[59]은 제외하고, 본 연구의 결론과 보다 논리적으로 밀접하게 연관될 수 있는 분류 기준을 중심으로 개인정보를 유형화하였다. 특정 개인에 대한 식별성 수준,

---

57) 정보통신망법에도 일반적인 개인정보의 수집 및 이용에 적용되는 조항 외에, 사상, 신념, 가족 및 친인척관계, 학력, 병력, 기타 사회활동 경력 등 개인의 권리 이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 원칙적으로 수집하여서는 안된다는 별도의 조항이 있다(제23조 제1항). 다만 정보통신망법은 강화된 규제가 적용될 필요가 있는 정보 항목들에 대하여 '민감정보' 등의 특정한 명칭을 부여하지 않으면서, 그 대상을 개인정보 보호법과 같은 방식으로 열거를 통해 특정하지 않았다는 점에서 선언적인 내용에 가까운 것으로 이해된다.

58) 인재근 의원 대표발의, 앞의 의안 제안 이유 중 아래 내용 참고
"4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 범국가적 과제로 대두되고 있으며, 특히, 신산업 육성을 위해서는 인공지능(AI), 클라우드, 사물인터넷(IoT) 등 신기술을 활용한 데이터 이용이 필요한 바, 안전한 데이터 이용을 위한 사회적 규범 정립이 시급한 상황임."

59) 예컨대 고유식별정보와 일반식별정보, 민감정보와 비민감정보, 사람정보와 정황정보, 사실정보와 평가정보, 배타적 정보와 비배타적 정보 등

개인정보가 수집된 출처 또는 경위, 개인정보 수집의 목적 등이 바로 위에서 말한 분류 기준에 해당하는데, 아래에서 차례로 소개하도록 하겠다.

제 2 절 식별성을 기준으로 한 분류

1. 식별성 요소에 관한 각종 쟁점

식별성 또는 식별가능성은 법상의 개인정보의 정의에서 직접적으로 발견되는 개념 표지이며("특정한 개인을 알아볼 수 있는"), 비교법적으로도 대부분의 입법례에서 개인정보를 구성하는 핵심적인 요소로 두고 있는 개념이다. 그럼에도 불구하고, 개인정보란 무엇인가에 대한 논의들이 사실상 대부분 식별성 또는 식별가능성의 개념에 대한 논의로 수렴되고 있을 정도로 '식별'이 무엇을 의미하는지, 언제 특정인이 '식별'되었다고 할 수 있는 것인지에 대한 풀이, 또는 개념에 대한 합의도 이루어져 있지 않은 것으로 보인다. 본 연구의 목적은 개인정보의 보호 범위를 합리화하려는 데 있으며, 개인정보의 개념 자체를 규명하고 그 의미 한계를 규명하는 것이 본래의 목적은 아니다. 따라서 아래에서는 선행 연구에서 되풀이하여 다루어져 온 식별성 개념에 대한 상세한 의미 분석 및 사례 연구보다는, 식별성을 기준으로 개인정보를 분류해보기 위한 전단계로서 식별성의 개념에서 문제되는 지점이 무엇인지에 대해 간략히 상술하도록 하겠다.

가. '식별'의 의미

정보통신망법 제2조 제6호는 '단독으로 개인을 알아볼 수 있는 정보'와 '다른 정보와 쉽게 결합하여 알아볼 수 있는 정보'를 개념상 구분하고 있다. 전자와 후자는 각각 '식별성'과 '식별 가능성'이라는 개념 표지로 압축되

는데, 특정 개인에 대해 어떠한 정보를 얻었을 때 해당 인물이 식별되는 것인지 의미가 명확하지 않다. 식별의 사전적 의미는 '분별하여 알아봄'이지만,[60] 통상적으로 당연히 개인정보에 해당하는 것으로 취급되는 성명의 경우를 예로 들어 볼 때, 특정인의 성명만을 안다고 하였을 때 해당 개인을 분별하여 알아보는 것이 가능한 것인지는 의문이다. 살아있는 다른 개인 중 동명이인이 존재하지 않는 등의 이례적인 경우를 제외하고, 성명만으로 해당 인물을 알아볼 수 있다고 확언하기는 어렵다.

그럼에도 불구하고 정보통신망법 제2조 제6호는 개인정보를 정의하면서 성명을 주민등록번호와 함께 특정한 개인을 알아볼 수 있는 정보의 대표격으로 언급하고 있어, 성명을 '단독으로 개인을 알아볼 수 있는 정보'로 보고 있는 것으로 이해된다. 주민등록번호의 경우 개인정보 보호법상 '고유식별정보'로 분류되어 있는 것과 걸맞게 단 1인에게만 대응되는 공적인 일련번호로서 특정인에게 바로 귀속되는 정보이기는 하나, 마찬가지로 다른 정보 없이 주민등록번호만을 안다고 하여서 해당 인물의 얼굴이나 이름을 알 수 있는 것도 아니다.

특정 개인을 '알아볼 수 있는' 정보란 무엇을 의미하는가에 대하여 행정안전부의 개인정보보호 법령 및 지침 고시 해설(이하 "개인정보 보호법 해설서")[61] 또는 국무조정실 등이 발간한 개인정보 비식별 조치 가이드라인(이하 "비식별조치 가이드라인")[62] 등에서는 식별의 주체를 누구로 보아야 하는가에 대해 설명할 뿐 언제 개인이 '식별'되는 것인지에 대해서는 명확히 설명하지 않는다.

상기 개인정보 보호법 해설서에서는 "주민등록번호와 같은 고유식별정보는 해당 정보만으로 정보주체인 개인을 알아볼 수 있지만, 생년월일의 경우에는

---

60) 표준국어대사전

61) 행정안전부, 개인정보보호 법령 및 지침 고시 해설(2016), 10.

62) 국무조정실·행정안전부·방송통신위원회·금융위원회·과학기술정보통신부·보건복지부, 개인정보 비식별 조치 가이드라인(2016), 4.

같은 날 태어난 사람이 여러 사람일 수 있으므로 다른 정보 없이 생년월일 그 자체만으로는 개인을 알아볼 수 있다고 볼 수 없다"고 하여 식별의 본래적인 의미가 특정인 1인의 신원과 직결되는, 일대일로 대응되는 정보 수준까지 확인하는 것을 가리키는 것처럼 풀이되어 있다. 반면 비식별조치 가이드라인에서는 개인정보를 구성하는 요소로서 식별자와 속성자를 구분하면서, 해당 정보만으로 특정 개인을 알아볼 수 있는 정보인지 아니면 결합을 요하는지를 기준으로 활용하며, 식별자의 예시로서 2명 이상의 사람에게 공통될 수 있는 성명, 생년월일 등은 물론 상세 주소나 각종 기념일 정보, 자격증 취득일 등까지 모두 포함시켜 두고 있기도 하다.

<표 3-1> 개인정보 비식별조치 가이드라인상의 `식별자'와 `속성자'의 구분

구분	식별자	속성자
개념	개인 또는 개인과 관련한 사물에 고유하게 부여된 값 또는 이름	개인과 관련된 정보로서 다른 정보와 쉽게 결합하는 경우 특정 개인을 알아볼 수도 있는 정보
예시	• 고유식별정보(주민등록번호, 여권번호, 외국인등록번호, 운전면허번호) • 성명(한자 영문 성명, 필명 등 포함) • 상세 주소(구 단위 미만까지 포함된 주소) • 날짜정보 : 생일(양/음력), 기념일(결혼, 돌, 환갑 등), 자격증 취득일 등 • 전화번호(휴대전화번호, 집전화, 회사전화, 팩스번호) • 의료기록번호, 건강보험번호, 복지 수급자 번호 • 통장계좌번호, 신용카드번호 • 각종 자격증 및 면허 번호	• 성별, 연령(나이), 국적, 고향, 시군구명, 우편번호, 병역여부, 결혼여부, 종교, 취미, 동호회·클럽 등 • 흡연여부, 음주여부, 채식여부, 관심사항 등 • 혈액형, 신장, 몸무게, 허리둘레, 혈압, 눈동자 색깔 등 • 신체검사 결과, 장애유형, 장애등급 등 • 병명, 상병(傷病)코드, 투약코드, 진료내역 등 • 세금 납부액, 신용등급, 기부금 등 • 건강보험료 납부액, 소득분위, 의료 급여자 등

	• 자동차 번호, 각종 기기의 등록번호 & 일련번호 • 사진(정지사진, 동영상, CCTV 영상 등) • 신체 식별정보(지문, 음성, 홍채 등) • 이메일 주소, IP 주소, Mac 주소, 홈페이지 URL 등 • 식별코드(아이디, 사원번호, 고객번호 등) • 기타 유일 식별번호 : 군번, 개인사업자의 사업자 등록번호 등	• 학교명, 학과명, 학년, 성적, 학력 등 • 경력, 직업, 직종, 직장명, 부서명, 직급, 전직장명 등 • 쿠키정보, 접속일시, 방문일시, 서비스 이용 기록, 접속 로그 등 • 인터넷 접속기록, 휴대전화 사용기록, GPS 데이터 등 • 배우자·자녀·부모·형제 등 가족 정보, 법정대리인 정보 등

식별의 개념에 대해서는 EU의 개인정보 보호를 위한 자문기구인 The Artcile Working Party(이하 'WP29')가 조금 더 구체적인 해석 또는 설명을 제시하고 있다.[63] WP는 2007년에 공식적으로 밝힌 의견을 통해, 특정 인물이 소속된 집단을 점점 좁혀 나감으로써 해당 인물을 다른 사람들과 구별(distinguished)할 수 있는 단계까지 도달하는 경우 이 때 식별된 것으로 볼 수 있다는 일반적인 설명을 제시하면서, 식별은 통상적으로 해당 인물과 관련하여 매우 특별하거나(privileged) 밀접한(close) 관계를 가지고 있는 식별자(identifier)를 통해 이루어진다고 설명했다. WP29는 이에 더하여, 흔한 성씨만을 가지고는 국가 수준에서 특정인을 식별해내기 어려운 반면 교실 내에서는 특정 학생을 식별해내는 것이 가능하다는 점을 예시로 들면서, 식별 가능성의 의미는 개인정보 처리를 전제하고 있는 상황(context)과 의존적인 관계에 있다는 점까지도 분명히 밝히고 있다.[64] 이와 같이 식별의 본질적인 요소를 집단 내에서의 구별 내지 구분으로

63) 이하 내용은 The Article Working Party, Opinion 4/2007 on the Concept of Personal Data (2007), 12-13 참조.

64) 상기 의견에서 WP29는 성명은 가장 일반적인 식별자(identifier)에 해당하며, '식별된 사람'이라는 개념은 흔히 해당 인물의 성명에 대한 언급을 암시하는 것이라고도 언급하고 있다(p13).

이해하고, 상황에 따라 식별의 수준을 다르게 볼 수 있다는 관점에 기반한다면, 반드시 특정인으로 수렴될 수밖에 없는 아주 높은 수준의 고유한 정보만을 식별정보로 볼 필요가 없게 된다.

결국 개인에 대해 어떠한 성격의 정보가 파악되어야 식별된 것으로 볼 수 있는지에 대한 명확한 결론은 없는 상태이나, 개인정보성이 문제되는 상황에 비추어, 사회통념상 해당 인물을 다른 사람들과 구분할 수 있는 기본적인 신원 또는 특질에 관한 정보가 파악되었다면 식별되었다고 해석할 수 있을 것을 보인다.[65]

○ EU에서 제시하는 식별성에 대한 평가 기준

한편, 국내법상의 개념은 아니지만 개인정보로서의 식별성과 관련하여 EU를 중심으로 빈번히 사용되고 있는 개념을 소개하고자 한다. 해당 개념은 식별성의 수준 자체를 정의하거나 또는 식별가능성의 정도에 따른 급간을 설정하는 것과 같이 식별 개념을 적극적으로 설명하기 위한 것은 아니다. 그보다는 식별성이 인위적으로 제거된 상태인 특정한 정보가 본래 의도한바와 같이 특정 개

"Concerning "directly" identified or identifiable persons, the name of the person is indeed the most common identifier, and, in practice, the notion of "identified person" implies most often a reference to the person's name."

65) 부연하여, 식별가능성을 누구를 기준으로 판단하느냐의 문제도 존재한다. 관련하여 개인정보분쟁조정위원회는 치아가 드러난 입모양이 확인되는 치아성형 전후 사진을 온라인상 무단 공개한 사안에서, 개인정보 보호법상의 개인정보 개념에 대해 "친분관계 등이 있는 사람이 특정 개인을 알아보는 것뿐만 아니라, 그 특정 개인을 전혀 모르던 사람이라도 객관적으로 그 특정 개인을 다른 사람과 구분·구별 할 수 있다면 모두 개인정보에 포함 될 수 있다는 의미"라고 판단하였다. 이에 의거할 때, 해당 사진만으로는 신청인을 모르던 사람이 신청인을 다른 사람과 구별 및 구분할 수 없다고 하며 해당 사진은 개인정보의 범위에 포함되지 않는다고 결정하였다 (개인정보분쟁조정위원회, 2013년 개인정보분쟁조정사례집(2013), 101 참조).

인을 식별하지 못하게 된 것이 맞는지 평가하는 과정에서 활용되는 개념 요소이다. WP29가 익명화 기술과 관련하여 의견을 공표하면서 해당 개념을 사용하였고, 정보가 완전히 익명화되었는지, 재식별의 위험이 없는지를 판단하기 위한 리스크 평가 기준으로서 Single out, Linkability, Inference라는 3개의 개념을 제시하였다.[66]

<표 3-2> 식별성에 대한 평가 기준

구분	개념	예시[67]
Single out	보유하고 있는 개인정보 항목 중 중 특정 개인 1인만을 따로 분리할 수 있는 정보인지 여부	개인의 신장에 관한 데이터 세트 중, 단 1인만이 190cm 이상인 경우 (또는 1990년대생 중에서는 단 1인만이 190cm인 경우) 해당 인물을 식별할 수 있음
Linkability	하나의 개인 또는 동일한 속성을 공유하는 집단에 관한 2개 이상의 데이터를 연결할 수 있는지 여부	이름이 A인 사람 또는 성이 B인 사람이라는 정보만을 각각 보유할 때보다, 전체 성명이 A와 B의 조합이라는 사실을 알 때 식별 가능성이 높아짐
Inference	2개 이상의 정보가 서로 정확하게 연결되어 있지 않더라도, 추론에 의해 연결 가능한지 여부	회사 내 직급 서열 관한 정보와 급여에 관한 정보가 별도로 존재할 때 2개를 합리적으로 추론하여 일부 개인이 식

66) The Article Working Party, Opinion 5/2014 on Anonymization Techniques(2014).
"Different anonymisation practices and techniques exist with variable degrees of robustness. This section will address the main points to be considered by data controllers in applying them by having regard, in particular, to the guarantee attainable by the given technique taking into account the current state of technology and considering three risks which are essential to anonymisation."

		별될 수 있음

나. 쉽게 결합하여

또한 개인정보에 대한 정의 중 “해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함”한다는 설명은 곧 식별가능성을 의미하는바, 식별의 의미가 1차적으로 규명되었다고 전제할 때, 식별가능성의 의미에서는 어떠한 경우에 2개 이상의 정보가 ‘쉽게 결합’된다고 볼 것인지가 핵심이 된다.

개인정보 보호법 해설서는 ‘쉽게 결합하여’(이하 ‘결합의 용이성’이라고도 칭함)는 “결합 대상이 될 정보의 입수 가능성이 있어야 하고 결합 가능성이 높아야 함”을 의미하며, “현재의 기술 수준을 고려하여 비용이나 노력이 비합리적으로 수반되지 않아야” 결합의 용이성이 인정될 수 있다고 설명하고 있다. 기술 수준에 입각하여 비용 및 노력의 투입이 필요한 정도를 고려하여야 한다는 것은 GDPR의 규정과도 일치한다.[68]

그러나 위와 같은 설명은 객관적인 난이도를 판단하는 최소한의 기준은 될 수 있으나, 결합의 용이성을 누구를 기준으로 판단하여야 하는지에 대해서는 구체적으로 방향을 제시하고 있지 않다. 이에 반해 일본의 개인정보의 보호에

---

67) 아일랜드의 개인정보 규제 당국인 Data Protection Commission 홈페이지상의 예시를 차용하였음. 아래 URL 참조
https://www.dataprotection.ie/docs/Anonymisation-and-seudonymisation/1594.htm

68) GDPR 전문 제26조 참조 (아래 관련부분 발췌)
“To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”

관한 법률에 관한 가이드라인은 “다른 정보와 용이하게 조합할 수 있다는 것은, 사업자의 실태에 맞게 개개 사례별로 판단되어야 할 것이나, 통상 업무에 있어서 일반적인 방법으로 다른 정보를 용이하게 조합할 수 있는 상태를 가리킨다. 예를 들어 타 사업자에게 조회하여야 하는 경우 등 조합이 곤란한 상태는 일반적으로 용이하게 조합할 수 없는 상태에 있는 것으로 풀이된다”고 명시하여,[69] 기본적인 판단 기준은 해당 개인정보처리자 및 정보통신서비스 제공자가 되어야 한다는 점을 명확히 하고 있다.[70] 다만 우리의 개인정보 보호법 해설서에서도 ‘입수 가능성’이라는 용어를 사용하고 있음을 볼 때, 결합의 용이성이라는 요건이 적어도 특정한 판단 주체를 전제하는 개념이라고 인식하

---

69) 日本 個人情報保護委員会, 個人情報の保護に関する法律ついてガイドラン(通則編) (2017. 3.), 10. 또한 해당 내용은 日本 総務省, 電気通信事業における個人情報保護に関するガイドライン(2017. 9.)에도 거의 동일하게 인용되어 있다.

“「他の情報と容易に照合することができ」るとは、事業者の実態に即して個々の事例ごとに判断されるべきであるが、通常の業務における一般的な方法で、他の情報と容易に照合することができる状態をいい、例えば、他の事業者への照会を要する場合等であって照合が困難な状態は、一般に、容易に照合することができない状態であると解される。”

70) 영국의 개인정보 관련 기본법인 Data Protection Act 1998의 경우, 개인정보의 정의 규정 자체에서 결합 대상 정보를 Data controller가 보관하고 있거나 또는 보관할 가능성이 있는 정보로 명시하고 있었다. (다만 해당 조항은 GDPR의 내용을 대폭 반영하며 지난 2018. 5. 새로이 시행된 신법(Data Protection Act 2018)에서는 다른 내용으로 수정되었다.)

“personal data” means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

고 있다는 것은 알 수 있다. 그와 달리 전지적인 관점에서 모든 사람이 보유하고 있는 개인정보를 대상으로 하여 정보들을 서로 연관 짓는 것이 용이한지 여부로 결합의 용이성을 판단하고, 그 결합을 통해 개인을 식별할 수 있는지의 여부로 개인정보성을 판단한다면, '쉽게'라는 한정적인 수식어는 개인정보의 개념 요건으로서 실질적인 의미를 갖기 어렵다.

그럼에도 불구하고, 국내 한 하급심 판결은 "쉽게 결합하여 알아볼 수 있다는 것은 쉽게 다른 정보를 구한다는 의미이기 보다는 구하기 쉬운지 어려운지와는 상관없이 해당정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다"고 판시한바 있다.[71] 위 판결은 이동통신 단말장치에 부여되는 고유 식별코드인 IMEI[72] 및 통신사 가입자 개인식별정보가 저장되어 있는 USIM카드의 일련번호에 대하여, 이동통신사가 보유·관리하고 있는 다른 인적 정보와 결합하면 특정 개인이 식별될 수 있다는 점에 근거하여 개인정보성을 인정하였다.

그런데 위 사안의 의 피고인은 이동통신사와는 무관한 모바일 어플리케이션 사업자였으며, 실제로 위 사안에서의 원고가 이동통신사가 보유하는 기타 개인정보를 용이하게 입수할 수 있었는지에 대해서는 구체적으로 논증하지 않았다.[73] 이동통신사의 전산시스템을 해킹하거나, 또는 다른 부정한 방법으로 정당한 권한 없이 시스템에 접근 또는 침입하는 것 외에는 이동통신사가 보관하는 IMEI, USIM 일련번호 정보와 연계된 다른 개인정보를 획득하는 것이 거의 불가능함에도 불구하고, IMEI나 USIM 일련번호와 특정 개인을 연결하는 정보가 실

---

71) 서울중앙지방법원 2011. 2. 23. 선고 2010고단5343 판결

72) International Mobile Equipment Identity를 말함

73) 이 사건에서 법원은 피고인 입장에서 결합이 용이하였는지에 관하여서는 "imei나 usim 일련번호와 관련된 개인에 관한 정보는 각 통신사별로 그 접근에 엄격한 통제를 가하고 있기는 하나, 제3자에 의하여 획득될 가능성이 없는 것으로 보이지는 아니"하다고만 언급한 후, "각 imei나 usim 일련번호는 휴대폰 가입신청서 등 가입자정보에 나타난 다른 정보와 어려움 없이 쉽게 결합"된다고 판시하였다.

제로 존재한다는 점만을 가지고 특정한 개인에 대한 식별가능성을 인정한 것이다. 결국 '쉽게 결합하여'라는 요건이 충족되는지에 관해서는, IMEI나 USIM과 결합하여 개인을 식별할 수 있는 정보가 어딘가에 존재한다는 점만을 근거로 판단을 한 것과 다름 없는데, 이러한 이유에서 위 판결은 그간 학계에서 많은 비판을 받아 왔다.[74]

관련하여 최근의 한 하급심 판결이 식별가능성에 관해 진일보한 판시를 내놓은 바 있어 향후 관련 법리의 발전에 대해 귀추가 주목된다. 해당 사건에서는 병원의 임직원들이 환자들의 혈액 샘플에서 '환자이름, 등록번호, 성별/나이, 병동' 부분은 삭제하고, '검체번호, 채혈시간, 검사항목, 검사결과 수치, 바코드' 부분을 남겨 제3자에게 전달한 것이 동의 없는 개인정보의 제3자 제공인지 여부가 문제되었다.[75] 이 사안에서는 병원 내의 시스템에서는 검체번호 등을 입력하는 방법으로 바로 환자의 인적 사항을 알 수 있었기 때문에, 병원을 기준으로 식별가능성을 판단한다면 검체번호 등의 개인정보성이 인정될 가능성이 매우 높았을 것으로 보인다. 그럼에도 법원은 어느 정보가 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 것인지 여부의 판단 기준에 대하여 "단순히 정보제공자를 기준으로 판단할 것이 아니라 해당 정보가 담고 있는 내용, 정보를 주고받는 사람들의 관계, 정보를 받는 사람의 이용목적 및 방법, 그 정보와 다른 정보를 결합하기 위해 필요한 노력과 비용의 정도, 정보의 결합을 통해 상대방이 얻는 이익의 내용 등을 합리적으로 고려하여 결정"하여야 한다고 판시하면서, 해당 자료를 전달받은 제3자가 환자의 구체적인 인적사항이 저장되어 있는 시스템에 접근할 권한이 없었으며, 접속 권한이 있는 병원의 임직

---

74) 이대희, "프로그램 포맷의 법적 위상과 보호방안에 관한 연구", 고려법학 제79호(2015), 180; 박민우, "개인정보 보호법상 불확정 개념에 있어 형법의 보장적 기능을 확인해주는 해석과 사회상규의 역할", 형사정책연구 제28권 제1호(2017), 91; 한국CPO포럼, 개인정보 관련 제재 및 피해구제 합리화 방안 연구(2013), 28 등.

75) 수원지방법원 2018. 4. 12. 선고 2017노7275 판결

원에게 인적사항 등에 관한 자료를 요청한 적도 없고, 해당 인적사항 정보가 필요하지도 않았다는 점 등을 근거로 검체번호 등의 정보가 '개인을 알아볼 수 있는 정보'에 해당한다고 볼 수 없다고 판시했다.

앞서 인용한 2010고단5343 판결의 논리구조를 차용할 경우, 2017노7275 판결 사안의 피고인들의 행위에 대한 법적 판단에 있어, 적어도 이들이 주고받은 정보가 개인정보에 해당하지 않는다는 결론은 내려지기 어려웠을 것으로 보인다. 2010고단5343 판결은 제3자에 의해 획득될 가능성이 없지는 않다는 이론상의 입수 가능성만을 근거로도 결합의 용이성을 인정하였는데, 2017노7275 판결에서는 실제로 개인정보를 바로 결합할 수 있는 접근권한이 있는 자로부터 해당 정보를 제공받은 것임에도 불구하고 개인정보의 내용, 개인정보 처리에 관여한 자들 간의 관계, 처리의 목적 등을 고려하여 결합의 용이성, 나아가 식별가능성을 부정한 것이다. 결합의 용이성에 관하여 실질적으로 판단을 하기 위하여서는 판단 주체의 문제를 간과할 수 없으며, 판단 주체를 설정하는 이상 '합리적인 비용 및 노력을 통해 개인 식별이 가능한지'에 대한 검토 과정에서 개인정보 처리의 목적이나 결합의 의도가 있는지 여부 등 주관적인 요건을 고려하지 않을 수 없다. 현재까지 개인정보 개념에 관한 국내의 판결례 중에서는 개인정보 처리의 목적과 의도 등을 적어도 중요하게 고려한 사례는 확인되지 않는바, 향후 판례의 축적을 통한 법리의 발전을 기대해 본다.

실제로 개인정보의 범위를 무한히 확장케 하는 실질적인 원인은 바로 이 식별 가능성 또는 결합의 용이성 개념을 명확히 한계짓기 어렵다는 점에 있다. 앞서 표 3-1로 인용한 개인정보 비식별조치 가이드라인상에서의 식별자와 속성자의 구분만을 보더라도, 식별자의 경우 누가 보더라도 일응 개인정보에 해당한다고 생각할 수 있는 것인 반면 속성자의 경우 어디까지가 개인정보인지 판단하기 애매한 것들이 대다수이다. 개인에 관한 정보에는 해당하는 것이 분명한 반면, 특정 개인을 구분 또는 구별해낼 수 있는 수준까지 이어지는지 여부가 명확하지 않은 것이다. 이 점에서 결합의 용이성을 어떻게 판단할 것이냐가

개인정보성의 논의에서 중요한 위치를 점하게 된다.

2. 식별성을 기준으로 한 개인정보의 분류

전술한 것과 같은 식별성에 관한 논의와 선행 연구들을 통하여 확립된 기준들을 종합하여, 개인에 관한 정보들은 식별성의 정도에 따라 일응 4가지 수준으로 분류하였다. 식별성을 기준으로 한 개인정보의 분류와 관련하여 유의하여야 할 점은, 어떠한 정보를 가지고 특정 개인을 식별할 수 있는가에 대해 검토하고 식별가능성 여부를 기준으로 정보들을 분류할 때, 단편적으로 해당 정보의 내용만을 고려하여서는 충분하지 못하다는 점이다. 앞서 살펴본 것과 같이 어떠한 정보가 개인정보에 해당하는지에 관하여 판단하는 과정에서는 해당 정보뿐 아니라 그와 결합할 수 있는 정보들까지 함께 고려된다. 특히 '결합할 수 있는 정보'는 어디엔가 존재한다는 것 자체로 족한 것이 아니라, 원칙적으로 합리적인 수준의 노력과 비용이 수반되는 범위 안에서 결합 가능할 때에야 식별성 판단 시에 함께 고려될 수 있다. 그렇다면 식별성의 유무 또는 고저에 관한 분류에 있어서도 내용뿐만이 아니라 결합이 현재 이루어져 있는지, 즉 어떠한 상태로 보관되어 있는지가 주요하게 고려되어야 할 것이다. 하며 본 연구서에서도 이 점을 고려하여 아래 나항과 다항을 서로 구분하였다.

가. 개인식별정보

개인식별정보라 함은, 다른 정보 없이 그 자체로 개인을 식별, 즉 다른 구성원과 구분해낼 수 있는 정보를 의미한다. 법상의 개인정보 정의규정에 직접 인용되어 있는 성명이나 주민등록번호가 그 대표적인 예시라고 할 수 있다. 다만 성명과 주민등록번호에 대하여도 식별의 의미를 어떻게 이해하는가에 따라 개인식별정보에 해당하는지에 관하여 다른 견해들이 제시된다. 예컨대 성명에 대하여 특정인을 직접 식별 가능한 정보로 보면서도 주민등록번호와 같은 고유식

별번호에 대해서는 개인이 속해 있는 그룹을 좁혀가면서 다른 식별요소들을 결합시킴으로써 간접적으로 식별할 수 있는 정보라고 보는 견해도 제시된다.[76]

어떠한 정보에 의하여 특정 개인이 식별되는가의 문제는 해당 정보가 처리되는 개별적인 배경과 상황과 완전히 분리하여 판단하기는 어렵기 때문에 개인식별정보의 범위를 사전에 일의적으로 획정하는 것은 논리적으로 가능하지 않다. 다만 특정한 인물을 직접 지칭하거나 또는 사회적으로 해당 인물을 구별 구분하기 위한 목적으로 부여된 정보는 일응 개인식별정보에 해당한다고 볼 수 있을 것으로 이해된다. 성명이나 주민등록번호는 이와 같은 관점에서 개인식별정보로 분류될 수 있을 것이다.

한편 이와 같이 특정 개인을 곧장 식별할 수 있는 정보를 '직접식별정보'라고 하고, 대조적으로 다른 정보와 결합하여 개인을 식별할 수 있는 정보를 '간접식별정보'로 칭하는 분류 사례도 발견된다. 다만 식별성이 가장 높은 정보 중 하나인 성명의 경우도 동명이인이 있을 수 있듯이, 직접식별정보는 이론적으로 존재할 수 있으나 실제로는 존재하기 어려우며 적어도 두 세 개 이상의 정보가 결합되어야 식별 가능한 개인에 관한 정보라고 할 수 있다는 점에 근거하여, 수 개의 정보가 결합되어 개인을 식별 가능한 상태에 이르면 해당 정보들이 일체로 직접식별정보로 전환된다고 설명하는 견해가 주장되고 있다.[77]

나. 개인식별정보와 결합되어 있는 상태의 개인식별가능정보

그 자체로는 개인을 식별할 수 없지만 개인을 식별할 수 있는 정보와 결합하

---

76) 이대희, 앞의 논문, 193.
"일정한 그룹에서 특정인을 구별하는 식별자로는 이름과 같이 직접 식별할 수 있는 것과 전화번호, 차량등록번호, 사회보장번호, 여권번호처럼 개인이 속해 있는 그룹을 좁혀가면서 식별할 수 있는 중요한 요소를 결합시킴으로써 간접적으로 식별할 수 있는 것이 있다."

77) 이창범, 앞의 책, 21.

여 개인정보가 될 수 있는 정보를 개인식별가능정보[78]라고 지칭할 수 있을 것이다. 개인식별가능정보는 결합을 전제로 하는 개념이기 때문에, 상태에 따라 실제로 이미 개인식별정보와 결합되어 있는 상태의 개인식별가능정보와, 반대로 아직 개인식별정보와 결합되지 않은 상태의 개인식별가능정보로 나눌 수 있다.

개인식별정보와 결합되어 있는 개인식별가능정보의 예로는, 회원제로 운영되는 온라인 쇼핑몰의 고객정보 중, 성명과 결합되어 보관되어 있는 전화번호, 주소, 이메일주소, 결제 관련 정보, 구매 이력 등이 있을 수 있다. 또한 개인식별정보와 쉽게 결합 가능한 개인식별가능정보로는 이미 개인의 성명 등의 정보를 가지고 있는 정보통신서비스 제공자에게 서비스 이용 과정에서 이메일 주소[79]나 전화번호[80] 등을 추가로 알려주는 경우 등이 이에 해당한다. 다만 이와 같

78) 주로 미국 법령에서 사용되는 Personally identifiable information ("PII") 개념과는 구별되는 것으로서, 본 연구서에서는 그 자체로는 개인정보를 식별할 수 없는 정보들, 즉 앞서 설명한 직접식별정보와 간접식별정보의 구분 중, 결합을 통해 직접식별정보로 전환되는 간접식별정보를 가리킨다. 참고로 미국 국립표술기술연구소 (National Institute of Standards and Technology, NIST)는 2010년 발행한 Guide to Protecting the Confidentiality of Personally Identifiable Information에서 PII의 개념을 다음과 같이 설명하고 있다.
"개인식별정보란 어떠한 기관이 관리하는 개인에 관한 정보로서, (i) 이름, 사회보장번호, 출생연월 및 출생지, 어머니의 혼인 전 성명, 생체 인식 기록 등과 같이 개인의 신원을 구별하거나 추적하기 위해 사용될 수 있는 정보, 또는 (ii) 의료, 교육, 재정, 고용에 관한 정보와 같이 개인에게 연결되거나 연결될 수 있는 정보를 포함한다."

79) 은행담당자가 특정 금융상품의 가입고객에게 이메일을 발송하면서 실수로 해당 금융상품에 가입한 고객 32,277명의 성명, 주민등록번호, 이메일 주소 등의 정보를 첨부파일로 발송해 이메일을 수령한 고객들이 다른 고객들의 정보를 알 수 있게 한 사안에서, 법원은 이메일주소에 대해 "당해 정보만으로는 특정 개인을 알아볼 수 없을지라도 다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보"에 해당한다고 판시한바 있다(서울중앙지방법원법 2007. 2. 8. 선고 2006가합33062, 53332 판결).

80) 경찰공무원이 피고인에게 제보자 휴대폰 뒷자리 4자를 알려주어 개인정보

이 결합된 상태의 정보들은 개념상 당연히 개인정보에 해당하므로 개인식별정보와 분리하여 따로 취급할 실익은 없을 것으로 보인다.

다. 개인식별정보와 결합되어 있지 않은 상태의 개인식별가능정보

개인을 식별할 수 있는 정보와의 결합이 이루어지지 않은 상태로서, 기술적으로는 해당 개인식별가능정보를 실마리로 하여 다른 개인식별정보를 추적해내는 것이 기술적으로는 가능한[81] 정보를 의미한다. 예를 들어, 별도로 이용자의 개인정보를 수집 및 이용하지 않는 정보통신서비스 사업자가 뉴스레터 수신을 희망하는 이용자로부터 이메일 정보만을 수집하여 뉴스레터를 발송하는 서비스를 운영하는 경우 그 수집된 이메일주소, 또는 이용자가 온라인 서비스에 로그인하지 않은 상태에서 검색한 기록 등의 행태정보 등이 이에 해당한다. GDPR상 추가적인 정보의 사용 없이는 더 이상 특정 정보주체를 식별할 수 없도록 가공된 이후 상기 '추가적인 정보'와 분리하여 보관하는 등의 가명처리(pseudonymisation)[82]를 거친 정보(이하 "GDPR상의 가명정보")도 일응 이 유

보호법 위반으로 기소된 사안에서, 법원은 "휴대전화번호 뒷자리 4자에 그 전화번호 사용자의 정체성이 담기는 현상이 점점 심화되고" 있음을 전제로, "설령 휴대전화번호 뒷자리 4자만으로는 그 전화번호 사용자를 식별하지 못한다 하더라도 그 뒷자리 번호 4자와 관련성이 있는 다른 정보(앞서 언급한 생일, 기념일, 집 전화번호, 가족 전화번호, 기존 통화내역 등)와 쉽게 결합하여 그 전화번호 사용자가 누구인지를 알아볼 수도 있다"고 판시하였다(대전지방법원 논산지원 2013. 8. 9. 선고 2013고단17 판결).

81) 해당 개인식별가능정보를 다른 정보들과 분석 및 결합하여 종국적으로 개인을 식별할 수 있는 가능성조차 존재하지 않는 경우라고 한다면 아예 식별이 불가능한 정보로서 별도로 취급되어야 할 것이다.

82) GDPR 제4조 정의규정 (개인정보보호위원회 번역문)
(5) 가명처리는 추가적인 정보의 사용 없이는 더 이상 특정 개인정보주체에게 연계될 수 없는 방식으로 개인정보를 처리하는 것이다. 단, 그 같은 추가정보는 별도로 보관하고, 기술 및 관리적 조치를 적용하여 해당 개인정보가 식별된 또는 식별될 수 있는 자연인에 연계되지 않도록 해야 한다.

형에 해당한다고 볼 수 있다.[83]

결합되지 않은 상태의 개인식별가능정보를 개인정보로 볼 수 있는지에 대해서는 논란이 많다. 특히 개인정보의 활용을 핵심으로 하는 ICT 신산업과 관련하여, 개인정보에 대해 식별성을 인위적으로 제거 또는 감소하는 절차를 거쳐 동 유형과 같은 식별가능성 수준 및 보관 상태로 가공한 정보들이 빈번하게 활용되기 때문에, 개인정보의 보호를 강조하는 진영에서는 이러한 정보들도 모두 개인정보로서 빠짐 없이 보호가 이루어져야 한다고 문제를 제기하는 경우가 종종 발생한다.

동 유형의 개인식별가능정보는 특정인과의 연결성을 유지하고 있는지 여부에 따라 다시 2가지로 분류할 수 있을 것으로 보인다. 신원을 알 수 없는 특정한 1인으로 정보들을 귀속시킬 수 있는 경우[84](이하 "1인으로 귀속되는 정보")와 그렇지 않은 경우는 별개로 보아야 하는데, 이는 전자의 경우 특정 개인을 식별할 수 있는 고리, 즉 결합만 이루어지면 1인으로 귀속되는 정보의 집단이 모두 개인정보에 해당할 수 있는 잠재적 식별성을 갖추고 있다고 볼 수 있기 때문이다.

<표 3-3> 1인으로 귀속되는 정보 및 1인으로 귀속되지 않는 정보의 구분

	1인으로 귀속되는 정보	1인으로 귀속되지 않는 정보
예시 · 설명	• ADID 등이 부여된 상태로 수집된 다양한 행태정보 • 여러 정보들 사이에서 특정인에 1인 대한 정보임을 구	• 로그인하지 않은 상태에서 수집된 행태정보로서 ADID를 부여하는 등으로 별도로 관리되고 있지 않은 정보

83) 다만 GDPR상의 가명정보의 경우, 노력이나 비용상의 문제로 결합이 어려운 것은 아니며 재식별, 즉 정보 사이의 결합에 대한 의도가 없기 때문에 식별성이 결여되는 것이라는 점에서는 완전히 동일하게 보기는 어려운 측면이 있다.

84) 이는 앞서 41면에서 EU에서 활용되는 재식별 위험 관련 평가요소 중 Single out의 의미와 유사한 것으로 이해할 수 있다.

	별할 수 있으나, 해당 인물이 누구인지 식별할 수 있는 정보는 결합되어 있지 않음	• 다만, 사업자가 원한다면 일정한 processing을 거쳐 Single Out을 하는 것이 가능한 경우일 것을 전제함

라. 개인을 식별할 수 없는 정보

마지막으로 개인을 식별할 수 없는 정보란, 개인식별정보와 결합될 수 있는 가능성조차 없는 정보(이하 “개인식별불가능정보”)를 의미한다. 예컨대 익명의 응답자에 대해 설문조사를 실시하는 과정에서 응답자의 신상에 관한 정보로는 연령대에 관한 정보만을 수령하는 경우 등이 이에 해당할 수 있다. 개인정보로 취급되지 않는 익명정보와 유사한 상태로 볼 수 있다. 개인식별불가능정보의 경우, 개념상 당연히 개인정보로 볼 수 없다는 점에 대해 대체로 견해가 일치하나, 기술의 발달로 인하여 모든 정보는 식별가능성을 가지고 있으므로 이와 같은 정보가 실재할 수는 없다는 견해도 제기되고 있다.

위와 같은 개인정보의 유형 분류는 앞서 언급한 것과 같이 정보 그 자체의 특성 및 내용적 측면만을 기준으로 한 것이 아니라 해당 정보가 관리되고 있는 ‘상태’를 기준으로 함께 고려한 것이다. 이와 관련하여 앞서 인용한 2017노7275 판결이 검체번호 등에 대하여 ‘개인을 알아볼 수 있는 정보’에 해당하지 않는다는 결론을 이끌어내기 위해 고려한 요소가 무엇인지를 다시 살펴볼 필요가 있다.

해당 사건에서 법원은 정보를 받는 사람의 이용목적 및 방법, 그 정보와 다른 정보를 결합하기 위해 필요한 노력과 비용의 정도, 정보의 결합을 통해 상대방이 얻는 이익의 내용 등을 합리적으로 고려하는 과정에서 사실상 개인정보의 보관 상태를 개인정보성의 판단기준으로 차용하였다. 해당 사건의 피고들이 검사정보시스템 프로그램에 접근할 수 있는 권한에 차등을 두면서 전자의무기

록 시스템은 전문의들만 접속할 수 있도록 관리하고 있었으며, 실제로 문제가 된 정보를 받은 업체가 피고인들에게 환자의 인적사항 등에 관한 자료를 요청한 적이 없을 뿐 아니라 검사정보시스템 프로그램에 접속한 적도 없는 점 등을 함께 고려하여, 위 정보를 개인정보로 볼 수 없고 검사의 공소사실에 대한 입증이 이루어졌다고 보기 어렵다고 판시하였다. 실제 사안에 대한 법원의 판단 과정에서도 대상 정보의 보관 상태가 식별성 유무를 판단하는 기준으로 활용되고 있는 것이다.

한편, 처음부터 개인을 식별할 수 없는 상태로 수집된 정보와, 처음에는 식별이 가능한 상태로 수집되었으나 사후적으로 식별성을 제거하는 가공 절차 (가명화 혹은 익명화)를 통해 식별성을 잃은 정보를 규제 측면에서 달리 볼 필요가 있는지가 문제될 수 있다. 예를 들어, 처음부터 로그인하지 않은 상태에서 수집된 검색어 입력 기록과, 로그인 상태에서의 검색기록이 수집되었으나 이후 기술적으로 계정정보와 분리되어 처리되는 경우를 달리 보아야 하는지의 문제가 이에 해당한다.

생각건대, 규제의 측면에서는 해당 개인정보의 처리가 이루어지는 특정 시점에서 앞서 구분한 식별성 정도에 따른 유형을 기준으로 규제를 적용하는 것으로 충분하며(예를 들어, 처음에 어떤 상태로 정보가 수집되었는지 불문하고 제3자 제공이 이루어지는 시점에서 해당 정보의 식별가능성을 판단), 결국 종국적인 판단 시점에 식별성 정도가 동일하다면, 최초의 상태를 기준으로 하여 규제 측면에서 달리 취급할 필요는 없을 것으로 생각된다.

제 3 절 수집 출처를 기준으로 한 분류

1. 수집 출처별 분류의 의미

개인정보를 수집 출처를 기준으로 분류하는 것도 가능하다. 이를 개인정보를

처리하는 사업자 등의 입장에서 보면 개인정보를 입수하게 된 구체적인 경로 또는 계기가 무엇인지의 문제가 된다. 현행법상으로는 개인정보를 어디서부터 수집해 왔는지의 문제는 그다지 큰 의미를 갖지 않는다. 단지 개인정보 보호법상 정보주체 이외로부터 수집한 개인정보에 대해 정보주체의 요청에 따라 개인정보의 수집 출처를 알려야 된다는 규정이 있을 뿐이다.[85] 그럼에도 불구하고 수집 출처를 기준으로 개인정보를 분류하는 것은 법적인 관점에서도 의미가 있다.

개인정보에 관한 권리가 비록 인격권에 뿌리를 두고 있는 개념이라고 하더라도, 자유로운 의사에 기한 사적 처분이 전혀 불가능한 권리라고 보는 것은 실제 권리 주체들의 인식이나 법 현실에도 맞지 않다. 개인의 기본권으로서의 인격권이 온전성을 훼손받지 않을 권리라고 한다면, "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리"로 풀이되는 개인정보자기결정권은 말 그대로 각 개인에게 결정권을 쥐어주는 기본권이다. 현대의 정보주체들은 누구나 자신의 개인정보를 부분적으로 처분하고 이를 적극적으로 활용하면서 사회적 관계를 형성하거나, 삶을 풍요롭게 하거나 또는 재산을 형성하는 데에 이용하고 있다.

이미 판례상으로도 수집 출처에 따라 개인정보 보호의 경중을 달리 보거나 개인정보 보호에 규제가 차등 적용될 수 있음이 인정된바 있다. 공개된 정보에 대하여는, 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서는 개인정보 처리에 대해 정보주체로부터 별도의 동의를 얻지 않아도 된다는 대법원

85) 개인정보 보호법 제20조

> 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.
> 1. 개인정보의 수집 출처
> 2. 개인정보의 처리 목적
> 3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

판결[86]이 바로 그것인데, 해당 사안에서 법원은 원고가 자발적으로 공개한 정보를 피고가 별도의 동의를 얻지 않고 영리 목적의 데이터베이스 서비스에 활용한 행위에 대해 개인정보 보호법 위반에 해당하지 않는다고 보았다. 물론 해당 사안의 경우 원고가 공립대학 교수라는 점에서 정보 활용이 공익적 이익에 기여할 수 있다는 측면도 함께 고려되었으나, 공개된 정보에 대해 최초 공개의 목적이 유지되는 범위 내에서는 개인정보 처리에 적용되는 일반적인 규제가 일부 배제될 수 있다는 점을 분명히 한 판결이라고 볼 수 있다.

개인정보에 관한 권리가 앞서 말한 것처럼 본인의 정보를 어떠한 범위에서 알리고 이용하도록 할 것인지 결정할 수 있는 권리라는 점을 고려할 때, 개인정보가 사업자 등에 수집된 경로나 계기 등에 비추어 얼마나 강하게 그러한 권리를 주장할 수 있는가에 차이가 있을 수 있다. 위 2014다235080 판결의 결론은, 누구나 접근할 수 있는 공개해 놓은 정보에 대해 다시금 당사자에게 적극적인 통제권을 인정하는 것은 부자연스럽다는 일반적인 상식 차원에서도 쉽게 이해할 수 있다.

---

86) 대법원 2016. 8. 17. 선고 2014다235080 판결
"정보주체가 직접 또는 제3자를 통하여 이미 공개한 개인정보는 그 공개 당시 정보주체가 자신의 개인정보에 대한 수집이나 제3자 제공 등의 처리에 대하여 일정한 범위 내에서 동의를 하였다고 할 것이다. 이와 같이 공개된 개인정보를 객관적으로 보아 정보주체가 동의한 범위 내에서 처리하는 것으로 평가할 수 있는 경우에도 그 동의의 범위가 외부에 표시되지 아니하였다는 이유만으로 또다시 정보주체의 별도의 동의를 받을 것을 요구한다면 이는 정보주체의 공개의사에도 부합하지 아니하거니와 정보주체나 개인정보처리자에게 무의미한 동의절차를 밟기 위한 비용만을 부담시키는 결과가 된다. 다른 한편, 개인정보보호법 제20조는 공개된 개인정보 등을 수집 처리하는 때에는 정보주체의 요구가 있으면 즉시 개인정보의 수집 출처, 개인정보의 처리 목적, 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알리도록 규정하고 있으므로, 공개된 개인정보에 대한 정보주체의 개인정보자기결정권은 이러한 사후통제에 의하여 보호받게 된다."

2. 수집 출처에 따른 개인정보의 분류

가. 이용자로부터 수집한 정보

이용자로부터 수집한 정보로 대표적인 것은 이용자가 서비스 이용 개시 및 회원 가입 과정에서 제공하는 개인정보가 있다. 또한 이용자가 입력한 검색어와 같이 서비스 이용 과정에서 제공하는 정보도 이 분류에 포함될 수 있다. 이용자로부터 수집한 정보의 경우, 이용자가 제공하지 않으면 알 수 없는 정보로서 이용자의 적극적인 행위를 통해 수집된다는 점에서, 이용자의 관점에서는 본인의 개인정보가 누군가에 의해 수집 및 이용되고 있다는 것을 비교적 쉽게 알 수 있다는 특성이 있다.

한편 본인뿐 아니라 제3자로부터 수집되는 개인정보도 존재한다. 예컨대 인터넷 상거래 서비스의 이용자가 제3자의 주소로 재화를 구매하는 경우라던지, 또는 본인의 소셜 네트워크 서비스 계정에 제3자의 사진을 업로드하는 경우 등이 이에 해당한다. 규제 측면에서 본인으로부터 직접 수집한 정보와 제3자로부터 수집한 정보를 달리 취급하여야 할 당위가 있다고 보기는 어려우나, 후자의 경우 정보주체로부터 직접 개인정보 처리에 대한 동의를 받거나 처리 사실을 알리는 것이 현실적으로 가능하지 않다는 점에서 사실적인 차이가 있다. 앞서 언급한 것처럼 개인정보 보호법의 경우 정보주체의 요구가 있을 때 수집 출처 등을 알려주어야 하는 방안으로 규제의 공백을 보완하고 있다.

나. 사업자가 생성한 정보

사업자가 본연의 업무 과정에서 필요에 의해 스스로 생성한 정보를 의미한다. 기존의 견해 중에서는 사업자가 생성한 정보와 생산한 정보를 구분하는 경우가 발견된다. 생성정보는 쿠키정보, 로그정보, 고객위치정보, IP 통신사실확인자료 등처럼 서비스과정에서 자동적으로 생성되어진 정보이며, 생산정보란 근

무평가, 신용평가, 인사기록, 진료차트, 비디오대여기록, 고객성향 등과 같이 개인정보처리자가 만들어낸 개인정보를 말한다는 것이다.[87]

이러한 구분 방식은 개인정보가 처리되는 방식 자체에 의미를 부여하는 규율 형태에서는 의미를 가질 수 있다. 예컨대 개인정보 처리방침상 "개인정보를 자동으로 수집하는 장치의 설치, 운영 및 거부에 관한 사항"을 포함하도록 하는 규제가 이에 해당한다.[88] 그러나 대부분의 정보처리가 자동화되어 있는 상황에서는 위와 같은 기준에 의거한 생성과 생산의 구분이 의미를 가지기 어렵다.[89] 사업자의 정보 처리 역량에 따라 어떤 사업자는 추가적인 노력을 들여 생산해내는 정보를 다른 사업자는 자동적으로 생성되도록 설정해놓을 수도 있다. 수집의 방식이 자동적이거나 수동적이거나 정보가 생성된 지배 영역이 이용자가 아닌 사업자측에 있다는 점, 그에 따라서 이용자는 본인의 개인정보가 수집 및 이용되고 있다는 점을 알기는 어려울 수 있다는 점, 이용자의 행위를 관찰하고 이를 집적 또는 구조화하거나, 평가하는 것이라는 점에서는 동일하다. 따라서 본 연구서의 목적에 비추어 볼 때, 사업자가 자동적 생성하는 정보와 생산하는 정보를 별도로 취급할 논리적 필요성은 없을 것으로 생각된다.

---

87) 김일환, "온주 개인정보보호법", 온주, http://www.onju.com/onju/service/writer/edit/SER_WEB03_1.aspx?lawid=243&lawtitle=%uAC1C%uC778%uC815%uBCF4%uBCF4%uD638%uBC95&commentid=0&lawnbId=00695240&decl=%uC81C1%uC870&state=0#76941|1|%uC81C2%uC870|3 (2018. 11. 1. 최종 확인); 이창범, 앞의 책, 22.

88) 정보통신망법 제27조의2 제2항 제6호, 개인정보 보호법, 개인정보 보호법 제30조 제1항 제7호

89) 박광배 외 2인, "빅데이터 시대 생성정보의 처리 체계", 정보법학(2017), 170.
"예컨대 OTT 서비스나 유튜브와 같은 자동화된 서비스에서라면 정보주체가 서비스 이용 과정에서 자동적으로 생성시키는 '생성정보'가 될 수 있을 것이기 때문이다. 학설이 '생산정보'의 범주에 포함시키고 있는 거래내역 및 실적 또한 마찬가지이다."

다. 공개된 정보를 수집한 정보

공개된 정보의 경우, 타인이 본인의 의사에 반하여 임의로 공개한 정보는 제외하고 본인이 최초에 목적과 범위를 적극적으로 인지한 상태에서 공개한 정보만을 의미하기 때문에, 실상은 가항의 “이용자로부터 수집한 정보”에 포함될 수도 있다. 다만 해당 정보를 이용하는 자의 관점에서는, 이미 개인정보로서 통상적인 보호 필요성을 일부 상실한 정보를 접하게 되는 것이므로 개인정보의 취급에서 구분할 필요가 있다고 본다.

제 4 절 목적을 기준으로 한 분류

또한 개인정보를 실제로 해당 정보가 이용되는 목적을 기준으로 분류하여보는 것 역시 가능하다. 사업자측의 이용 목적은 경우에 따라 천차만별이겠으나 극히 단순화하여 볼 때, 내부적인 이용 목적에서 그치는 경우와 정보주체를 포함한 외부에 노출시키거나 제공할 목적으로 분리하여 볼 수 있다. 예를 들어, 이용자에게 서비스를 제공하기 위해 수집한 이용자 계정 정보의 경우 전제에 속하며, 제3자 업체에게 맞춤형 광고를 의뢰하기 위한 목적으로 수집된 정보는 후자로 볼 수 있을 것이다.

개인정보가 외부로 제공되는 경우, 본인의 개인정보의 유통에 대한 통제권 내지는 알 권리 등은 점점 더 약화될 수밖에 없다. 모든 이용자가 굉장히 높은 개인정보 감수성을 지니고 있을 것으로 기대하기 어려운 상황에서, 이용자가 직접 서비스 이용 관계 등을 맺고 있는 상대방 당사자인 사업자가 아니라 한 단계를 더 거치는 완전한 타인에 대하여까지 적극적으로 통제권을 행사하기는 어렵다. 이 점에서 외부에 제공되는 개인정보는 태생적으로 위험도가 높을 수밖에 없으며, 현행법상 개인정보의 제공에 대하여 수집 및 이용과는 반드시 별도로 동의하여야 할 대상으로 두면서, 이에 동의하지 않아도 서비스 이용이 가

능하여야 한다고 명시하고 있는 것도 동일한 맥락으로 이해된다.[90]

따라서 외부 제공 목적인 개인정보에 대하여는 규제의 필요성이 보다 크다고 할 수 있다. 특히, 앞서 언급한 수집 출처에 따른 분류까지 함께 고려하할 때, 사업자가 생성한 정보가 내부적으로만 활용된 이후 파기되는 것이라면 규제의 필요성은 매우 낮다고 할 것이다. 예를 들어, 사업자가 이용자의 불만 내지는 민원에 대응하는 과정에서, 내부적인 업무 관리를 위해 임의적으로 부여한 민원 처리 번호를 예시로 들 수 있다. 이러한 정보는 사업자가 보유하고 있는 이용자의 개인식별정보나, 민원의 내용이나 사용하고 있는 서비스 품목 등 기타의 개인식별가능정보 결합하여 개인정보에 해당할 수 있으나, 외부에 노출될 가능성 내지는 가치가 전혀 없이 내부적으로만 이용할 목적에 그친다는 점에서 규제의 필요성이 매우 낮다고 볼 수 있다.

90) 정보통신망법 제24조의2

> 제24조의2(개인정보의 제공 동의 등)
> ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. (중략)
> ③ 제25조제1항에 따른 정보통신서비스 제공자등은 제1항에 따른 제공에 대한 동의와 제25조제1항에 따른 개인정보 처리위탁에 대한 동의를 받을 때에는 제22조에 따른 개인정보의 수집·이용에 대한 동의와 구분하여 받아야 하고, 이에 동의하지 아니한다는 이유로 서비스 제공을 거부하여서는 아니 된다.

제 4 장 규제 유형별 차등적 해석 가능성

제 1 절 개인정보 관련 규제에 대한 접근 방법

1. 개인정보의 보호와 이용

개인정보 보호법은 공공기관개인정보보호에관한법률의 폐지와 동시에 공공과 민간 부문의 개인정보 보호를 통합하여 규율하여 온 반면, 정보통신망법상의 개인정보 관련 규정들은 기본적으로 영리 목적의 사업자가 제공하는 정보통신서비스의 이용촉진을 목적으로 하던 법률에 개인정보의 오·남용 등 부작용을 방지하기 위한 목적으로 관련 규제가 신설되는 방식으로 처음 등장하였다.[91] 개인정보의 상업적 활용을 요소로 하는 서비스의 이용을 촉진하면서 동시에 그 과정에서의 개인정보 보호를 규율하는 정보통신망법의 규정에 대해서는 보호와 이용 중 한쪽이 불필요하게 축소되지 않도록 하는 균형이 필요하다.

설령 개인정보 보호법만이 적용되는 경우라고 하더라도 보호가 이용을 압도하는 절대적인 가치는 될 수 없다. 오늘날과 같은 정보화 사회 내지 초연결 사회에서는 개인정보의 자유로운 유통에 의한 편익을 오로지 기업의 이윤 취득이라는 관점에서만 볼 수 없다. 시장경제 속에서 올바른 결정과 판단을 내리기

---

91) 정보통신망이용촉진등에관한법률 (법률 제5835호, 1999. 2. 8., 전부개정)의 제·개정이유 중 발췌

◇개정이유

정보통신망을 통하여 수집·처리·보관·유통되는 개인정보의 오·남용에 대비하여 개인정보에 대한 보호규정을 신설하고, 수신자의 의사에 반하여 광고성 정보를 전송하는 행위를 금지하며, 한국전산원의 설립에 관한 사항등을 정보화촉진기본법으로 이관하는 등 정보화촉진기본법과의 관계를 재정비하는 한편, 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하려는 것임.

위하여 불확실성은 가능한 한 줄이고, 필요한 정보를 가능한 한 많이 획득하여야 하기 때문에, 시장경제가 제대로 기능하기 위해서는 부분적으로 또는 분야별로 개인정보보호가 요구되기도 하나 이와 동시에 개인관련정보의 가능한 한 방해받지 않는 접근과 광범위한 저장 및 이용자유를 전제로 한다는 분석도 이루어지고 있다.[92]

이와 같이 국가의 기능을 포함한 온갖 사회적 기제가 정보의 수집, 이용, 분석 등을 포함하지 않고 운영되는 것이 없으며 개인정보의 활용에 따른 편익은 이미 충분히 경험되고 있다. 무엇보다 그러한 편익과 개인정보가 권한 없는 제3자에게 노출되는 경우의 폐해 등을 양자택일의 문제로 볼 이유가 없다. 개인정보 보호에 관한 법령들을 해석 및 적용함에 있어서는 보호와 이용의 가치가 함께 충분히 고려되는 적절한 균형을 도모하여야 하며, 해외의 개인정보 보호 법령들도 공통적으로 보호와 이용의 균형을 도모하고 있다.[93] 부가가치 및 이윤 창출이 가능한 정보자산으로서 개인정보의 가치가 강조되는 시대의 정보통신 관련 법령의 경우에는 이용의 측면이 보다 적극적으로 고려될 필요가 있다.

소위 4차 산업혁명의 시대가 도래하면서 국내의 각종 법제 가운데 가장 먼저 개인정보 보호 관련 규제의 개선 필요성이 지적될 정도로, 데이터 및 개인정보 활용은 ICT 신산업에 있어서 경쟁력의 원천이다. 이에 그간 개인정보의 보호에 치중되어 있던 정책적 화두가 이용과의 사이에 균형을 찾는 방향으로 조금씩 변모하고 있는 모습이 발견된다. 그러한 균형을 회복하기 위하여서는 먼저 보호와 이용 사이에 존재하는 긴장관계에 대한 정확한 이해가 필요하다. 개인정보의 이용이 활성화되어야 하는데 그 목적은 ICT 신산업의 발전이고 이를 위해서는 개인정보의 이용이 필수불가결하다는 식의 접근은 그 자체로서 아무런 논리를 포함하지 못하는 순환논리에 불과할 뿐 아니라, 이용의 범위를 어디까지

92) 김일환, "개인정보의 보호와 이용법제의 분석을 위한 헌법상 고찰", 헌법학연구 제17권 제2호(2011), 362.

93) 이인호, "「개인정보 보호법」상의 '개인정보' 개념에 대한 해석론", 정보법학 제19권 제1호(2015), 66.

보장하여야 하고 그 근거는 무엇인지 등에 대한 발전적인 논의를 가능케 할 수 없기 때문이다.

2. 보호와 이용의 관계에 대한 법리적인 이해

가. 정보주체와 사업자의 기본권의 충돌

정보통신서비스 제공자와 그 이용자 사이에는 계약관계가 존재한다. 사업자가 사전에 마련한 약관에 명시적으로 동의를 하였든, 아니면 단순히 서비스 이용 과정에서 동의의사가 묵시적으로 표현되든 이용자는 일상적으로 교통수단을 이용하는 것과 마찬가지로 정보통신서비스를 이용하면서 사업자와 계약관계를 맺는다. 계약관계 내에 존재하는 급부의 제공과 그에 부수되는 거래 등은 원칙적으로 모두 계약 자유의 원칙 또는 사적 자치의 원칙의 지배를 받으므로, 정보통신서비스 제공자가 계약 관계에서 이용자 본인으로부터 동의를 얻어 취득한 개인정보를 처리하는 것에 대하여도 사적 자치에 따르는 것이 원칙이다.

그러나 사적 자치의 원칙은 그로부터 발생하는 폐해 또는 부작용 등을 교정하기 위한 강행법규에 대해서는 열위에 있다. 개인정보 처리와 관련하여서는 개인정보의 무분별한 오남용을 막기 위하여 정보통신망법의 규율이 강행법규로 기능하고 있으므로, 정보통신망법이 이용자의 정보통신서비스 이용관계에 적용되어 각종 의무를 부담하게 되는 것이다.

특히 정보통신서비스 제공 과정에서의 개인정보 처리 또는 그에 관한 계약은 집단적, 반복적으로 대량으로 행해지며, 매우 신속하게 처리되는 특징이 있다. 이러한 점을 고려하여 정보통신망법은 개인정보 보호법에 비하여 보다 규율을 강화하고 이용자의 권리를 보다 강조하고 있다. 열람청구에 있어 개인정보의 열람 제공 내역을 법에서 직접 특정하고 있고,[94] 개인정보의 이용내역을 연 1

94) 개인정보 보호법 제35조 및 정보통신망법 제30조

개인정보 보호법 제35조(개인정보의 열람)

회 이상 이용자에게 통지하도록 하고 있기도 하다.

이와 같이 본래 사적 자치 및 계약의 영역에 속하는 민간 부문의 개인정보 처리에 대하여 법상의 개인정보 보호를 위한 조치가 의무화됨으로써, 영리추구를 위하여 개인정보를 활용하고자 하는 수범자들은 기업 활동의 범위를 제약받는 결과가 된다.[95] 이를 기본권의 관점에서 살펴보면, 사업자의 입장에서는 헌법 제15조에 의하여 보호되는 직업수행의 자유, 즉 본인이 선택한 직업 또는 영업을 원하는 방식으로 자유롭게 수행할 수 있는 자유를 제한받는 것이 된다.[96] 이용자의 개인정보자기결정권을 보호하기 위해 또 다른 기본권 주체의

---

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

정보통신망법 제30조(이용자의 권리 등)
② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.
1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

95) 황성기, 앞의 논문, 25.
"사업자들은 개인정보 보호법이나 정보통신망법상의 개인정보 보호관련 규정들에 근거해서 개인정보 보호를 위하여 인적 물적 비용 등을 투입하고 있다. 실제로 개인정보 보호를 위한 인적 비용으로 개인정보 보호책임자(Chief Privacy Officer: CPO)와 본부 단위의 팀이 투입되고 있으며, 개인정보보호법상의 기술적 관리적 및 물리적 보호조치의무에 따라 물적 비용으로 보안시스템 구축 및 유지 비용, 매년 이루어지는 실태조사에 따른 비용, 관제서비스 구축(시스템 공격에 대한 방어)에 따른 비용 등이 투입되고 있다. 더 나아가서 개별 사업자들은 개인정보보호법이나 정보통신망법상의 개인정보 보호관련 규정들이 너무 강력하여 고객관리 및 리스크관리에 어려움이 많을 뿐만 아니라, 비즈니스의 창의성이나 다양성을 확보하기 어렵다는 호소를 많이 한다."

기본권을 제한하는 이와 같은 상황은 헌법상으로는 개인정보 충돌로 풀이된다. 이와 같이 2개의 기본권이 서로 충돌하는 상황에서의 해결방안에 대해, 헌법재판소는 헌법의 통일성을 유지하기 위하여 상충하는 기본권 모두가 최대한으로 그 기능과 효력을 발휘할 수 있도록 조화로운 방법을 모색하되(이른바 규범조화적 해석), 법익형량의 원리, 입법에 의한 선택적 재량 등을 종합적으로 참작하여야 한다고 판시한바 있다.[97]

다시 말하여, 개인정보자기결정권 역시 한계가 없이 무한정 보장되는 권리가 아니므로, 개인정보자기결정권을 보장 및 보호하기 위한 법률상의 장치는 타인의 기본권과 조화를 이룰 수 있는 범위 내에서만 합헌적일 수 있으며, 그 판단을 위하여서는 두 기본권 주체의 침해되는 법익의 내용 및 정도 등을 형량해 보아야 한다는 것이다.[98] 이러한 기본적인 원칙은 GDPR에서도 마찬가지로 언급되고 있다. GDPR은 전문 제4조에서 개인정보의 보호에 대한 권리는 절대적인 권리가 아니며, 비례성의 원칙에 따라 다른 기본권과 균형을 이루어져야한다는 점을 명시하면서, 함께 균형을 이루어야 할 권리로서 사업을 수행할 자유

---

96) 법인도 성질상 법인이 누릴 수 있는 기본권의 주체가 되는데, 직업의 자유는 헌법상 법인에게도 인정되는 기본권이다. (헌법재판소 2002. 9. 19. 선고 2000헌바84 결정 등)

97) 헌법재판소 2005. 11. 24. 선고 2002헌바95, 96, 2003헌바9 결정.

98) 이 때 이루어지는 이익형량의 내용은 다음과 같다. (보험회사 직원이 보험회사를 상대로 손해배상청구소송을 제기한 교통사고 피해자들의 장해 정도에 관한 증거자료를 수집할 목적으로 피해자들의 일상생활을 촬영한 행위의 위법성에 대해 판단한 대법원 2006. 10. 13. 선고 2004다16280 판결 등)
"이러한 이익형량과정에서, 첫째 침해행위의 영역에 속하는 고려요소로는 침해행위로 달성하려는 이익(이하 '침해법익'이라 한다)의 내용 및 그 중대성, 침해행위의 필요성과 효과성, 침해행위의 보충성과 긴급성, 침해방법의 상당성 등이 있고, 둘째 피해이익의 영역에 속하는 고려요소로는 피해법익의 내용과 중대성 및 침해행위로 인하여 피해자가 입는 피해의 정도, 피해이익의 보호가치 등이 있다. 그리고 일단 권리의 보호영역을 침범함으로써 불법행위를 구성한다고 평가된 행위가 위법하지 않다는 점은 이를 주장하는 사람이 증명하여야 한다."

(freedom to conduct a business) 역시 언급하고 있다.[99] [100]

대법원 역시 기본권의 충돌이 분쟁으로 구체화된 사안에서 유사한 법리를 적용하여 판결을 내리고 있다. 대표적인 사안으로, 법률정보 제공 사이트를 운영하는 사업자가 공립대학교 법과대학에 교수로 재직 중인 자의 사진, 성명, 성별, 출생연도, 직업, 직장, 학력, 경력 등의 개인정보를 학교 홈페이지 등을 통해 수집하여 상기 웹사이트의 '법조인' 항목에서 유료로 제공한 사건에서, 사업자가 정보주체의 동의 없이 개인정보를 본인이 운영하는 웹사이트에 게재한 것이 개인정보 보호법을 위반한 행위인지 여부가 쟁점이 되었다.

대법원은 위 사건에 대한 판단 부분에서 "개인정보에 관한 인격권 보호에 의하여 얻을 수 있는 이익과 그 정보처리 행위로 인하여 얻을 수 있는 이익 즉 정보처리자의 '알 권리'와 이를 기반으로 한 정보수용자의 '알 권리' 및 표현의 자유, 정보처리자의 영업의 자유, 사회 전체의 경제적 효율성 등의 가치를 구체적으로 비교 형량하여 어느 쪽 이익이 더 우월한 것으로 평가할 수 있

---

99) Recital 4 Data protection in balance with other fundamental rights
The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

100) 사회·경제활동의 자율과 창의를 촉진하여 국민의 삶의 질을 높이고 국가경쟁력이 지속적으로 향상되도록 함을 목적으로 하는 행정규제기본법 제5조 역시 "국가나 지방자치단체는 국민의 자유와 창의를 존중하여야 하며, 규제를 정하는 경우에도 그 본질적 내용을 침해하지 아니하도록 하여야 한다."는 규제의 원칙을 정하고 있다.

는지에 따라 그 정보처리 행위의 최종적인 위법성 여부를 판단하여야" 한다고 판시하였다.[101] 즉 개인정보에 대한 보호 범위를 획정하는 데에는 그 반대편에 있는 정보통신서비스 사업자의 영업의 자유의 보호 필요성을 함께 고려하여야 한다는 것을 분명히 한 것이다.

나. 데이터에 대한 기업의 권리

나아가, 위와 같은 법익 형량의 과정에서 반드시 고려하여야 할 측면이 데이터에 대해 기업이 갖는 권리이다. 이는 특히 사업자가 생성한 정보와 관련이 깊은데, 근래 IoT, 빅데이터, AI 등 정보기술 발전이 촉진됨에 따라 데이터는 기업의 경쟁력의 원천이라는 점을 배경으로 최근 EU, 일본 등에서 '데이터'의 소유(ownership) 및 통제권을 보장하고자 하는 입법 작업 및 연구가 시작되었다.[102] 일본에서는 부정경쟁방지법을 개정하여 영업비밀에 이르지 않는 '데이터'에 대하여도 별도로 보호를 위한 규율을 도입하였으며,[103] EU는 유럽집행

---

101) 대법원 2016. 8. 17. 선고 2014다235080 판결. 대상 판결은 위와 같은 판단에 있어서는 정보주체가 공적인 존재인지, 개인정보의 공공성과 공익성, 원래 공개한 대상 범위, 개인정보 처리의 목적·절차·이용형태의 상당성과 필요성, 개인정보 처리로 인하여 침해될 수 있는 이익의 성질과 내용 등 여러 사정을 종합적으로 고려하여야 한다고도 하였다.

102) 국내 문헌에서의 유사한 언급으로는 한국인터넷법학회, 개인정보 보호와 적정 활용의 조화를 위한 제도 도입 연구(2009), 44 참조.
"반면 개인정보의 경제적 가치를 중시하는 입장에서는 개인정보를 기업의 마케팅 능력 강화를 위해서 수집 활용될 수밖에 없는 필수의 영업자산 또는 자원으로 생각한다. 이들은 사업자가 상업적 목적으로 소비자의 개인정보를 수집·이용하는 것은 시중에 떠도는 소문이나 정보를 수집해서 영업활동에 활용하는 것과 다를 게 없다고 주장하며, 한 개인의 구매습관에 관한 정보는 상품의 구매자인 소비자 자신뿐만 아니라 상품 판매자인 사업자의 소유에 속한다고 주장한다."

103) 2019. 7. 1. 시행 예정인 일본의 부정경쟁방지법은 '한정제공데이터'라는 개념을 신설하면서 영업비밀에 이르지 않는 기업 내에 축적된 정보를 부정취득행위로부터 보호하는 새로운 규율을 도입했다. 일본 경제산업성이 개

위원회의 연구혁신프로젝트의 일환으로서 “White paper on Data Ownership104)”을 발표하면서, 데이터에 대한 사업자의 통제 및 권리에 영향을 줄 수 있는 수많은 법률이 확인됨에도, 데이터 소유권에 대해 정하는 법률은 없다는 점을 꼬집기도 하였다.

사업자가 자신의 창의를 더하여 어떠한 정보를 생성하였을 때, 해당 정보의 원재료가 이용자의 개인정보라고 하여 개인정보 관련 규제가 무제한 적용되어야 하는가에 대한 의문은 일견 합당해 보인다. 때로는 사업자가 어떤 기술을 사용하여 새로운 생성한다는 것까지 알지 못하더라도, 어떠한 종류의 개인정보를 생성해낸다는 것 자체가 중대한 영업비밀을 함축하는 것일 수 있다. 이와

정 부정경쟁방지법의 취지에 대해 설명하기를, IoT, 빅데이터, AI 등 정보기술이 발전하는 4차 산업혁명을 배경으로 데이터가 기업 경쟁력의 원천으로서의 가치가 증대되고 있으며, 기상데이터, 지도데이터, 기계가동데이터, 소비동향데이터 등은 공유, 이용 및 활용되어 새로운 사업과 고부가가치가 창출되고 있다는 점, 그러나 데이터는 복제가 용이하고 일단 부정하게 취득된 데이터는 대량으로 확산되기 쉬운 특성이 있으며 기존 법률로는 데이터를 보호 및 활용하기 어렵다는 우려가 있다고 밝혔다.

한정제공데이터: 업으로서 특정인에게 제공하는 정보로서 전자[電磁]적 방법(전자[電子]적 방법, 자기적 방법 기타 타인의 지각에 의해서는 인식할 수 없는 방법을 말한다. 다음 항에 있어서 같다.)에 의하여 상당량 축적 및 관리되는 기술상 또는 영업상의 정보(비밀로서 관리되고 있는 것을 제외한다.)

104) Bird & Bird, Data Ownership - Building the European Data Economy(2017). 또한 이 백서는 GDPR은 데이터의 소유 또는 개인정보에 대한 상업적 이용에 관한 권리에 대해 다루지 않는다는 사실을 언급하면서, 어떠한 정보가 개인정든 아니든 그 소유권의 문제는 데이터 컨트롤러 또는 프로세서가 사실상 소유하고 있는 정보에 대해서 검토될 수 있으나, 정보주체는 GDPR의 적용범위 내에서 개인정보에 대한 통제를 유지하게 된다는 것을 전제로 하고 있다고 명시하고 있다. (“The present specific report takes an approach whereby ownership is examined in relation to data, be it non-personal or personal data, which can be as a matter of fact owned by data controllers or processors but where data subjects maintain a control over their personal data within the limits of the GDPR.”)

같은 정보들을 예외 없이 이용자의 개인정보 처리 내역으로서 열람권 행사의 대상으로 보아 외부에 유출하도록 강제한다면, 이는 사업자의 관점에서는 영업의 자유에 대한 과도한 제한이 될 수 있다.

이와 같이, 개인정보의 보호와 이용의 관점이 서로 충돌하고, 개인의 개인정보자기결정권과 사업자의 자율과 창의가 서로 충돌하는 상황에서는 개인정보에 대한 보호뿐 아니라 사업자의 영업의 자유나 영업비밀 또는 재산권적 가치 있는 보유 정보에 대한 보호가 충분히 고려되어야 하며, 정보통신망법의 각 규율에 대한 해석 및 적용 역시 이러한 균형잡힌 시각에 기초하여 행해져야 한다.[105]

3. 개인정보에 관한 통제권의 의미 및 범위

앞서 제2장에서 언급한 것과 같이, 오늘날 개인정보에 관한 권리는 "자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리"로 이해되고 있으며, 법상 사업자에게 부과되는 다수의 의무들은 대부분 위와 같은 통제권을 보장하기 위한 도구이다. 문제는 통제의 권리가 실제 이용자의 권리 행사에서 어느 정도까지 발현 또는 보장되어야 하는지가 명확하지 않다는 점이다.

개인정보라는 것은 그 주인에게 머무르는 것이 아니라, 정보의 태생적 속성에 따라 정보주체와 타인간의 사회적 관계 속에서 유통되며, 그러한 유통과 활용 과정에서 적절한 보호만 주어진다면 정보주체나 그와 관계를 맺는 거래상대방, 나아가 사회 전반에 편익을 가져다 준다. 이와 같이 유통되는 정보의 특성상, 일단 통제권자의 절대적인 지배영역을 벗어나 전전유통되기 시작하면, 최초에 그 정보를 보유하고 있던 사람이 정보에 대해 계속하여 통제권을 행사한다는 것은 상당히 부자연스럽다. 통제권의 행사와 개인정보의 원활한 이용은 서

105) 이와 같은 이익형량의 필요성에 대해 강조한 논문으로는 채성희, "개인정보자기결정권과 잊혀진 헌법재판소 결정들을 위한 변명", 정보법학 제20권 제3호(2016) 참조.

로 대척점에 존재한다는 의미이다. 때문에 통제권의 의미를 매우 적극적인 형태로 이해한다면 그만큼 개인정보의 이용촉진 측면은 저하될 수밖에 없다. 앞서 예시로 든 사업자의 영업비밀이 함축된 개인정보 생성 내역에 대한 열람제공의무가 바로 그러한 예이다.

개인정보자기결정권에 포함되어 있는 통제의 요소가 어떻게 해석되어야 하는지는 결국 개인정보자기결정권의 보장 근거에 비추어 검토되어야 한다. 앞서 소개한 대법원과 헌법재판소의 판결 및 결정례에서는 개인정보자기결정권의 헌법적 근거에 대하여 조금씩 다르게 설명하고 있다. 대법원은 96다42789판결에서 개인정보자기결정권의 근거를 헌법 제10조의 인간의 존엄과 행복추구권, 그리고 헌법 17조의 사생활의 비밀과 자유에서 찾고 있으며,[106] 헌법재판소의 경우 99헌마513 결정에서 사생활의 비밀과 자유, 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권, 자유민주적 기본질서와 국민주권 민주주의 원리에 고루 근거한 독자적 기본권이라고 판시하기도 했다. 다만 이후 결정에서는 헌법 제10조 제1문의 일반적 인격권 및 제17조 사생활의 비밀과 자유에서 근거를 찾는 등[107] 그 근거를 일관되게 제시하고 있지는 않다.

생각건대 개인정보자기결정권은, 그 처리 주체가 국가이든 또는 기업이든을 불문하고 대량의 정보를 축적할 능력이 있는 제3자에 대하여 개인이 본인의 인격상이 총체적으로 타인의 수중 하에 넘어가지 않도록 할 수 있는 장치를 보장

---

106) 동 판결에서 대법원이 “개인정보자기결정권”이라는 용어를 직접 사용하고 있는 것은 아니다. 다만 뒤이어 2014. 7. 24. 선고 2012다49933판결에서 아래와 같이 개인정보자기결정권이라는 용어를 사용하면서, 그 헌법적 근거에 대해서도 명확히 하였다.
“인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장되는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다.”

107) 헌법재판소 2005. 7. 21. 선고 2003헌마282 결정

함으로써, 자유로이 자신의 인격을 발현하고 주체로서 행동할 수 있는 자유를 보장하는 것으로 이해된다. 정보주체가 스스로의 정보를 타인에게 노출시키거나 공유할 의향이 전혀 없는 상황만을 전제한다면 사생활의 비밀의 자유 역시 개인정보를 보호에 대한 부분적인 근거가 될 수 있을 것이나, 정보주체의 사회적 활동과 관계를 전제한 상태에서의 개인정보 보호를 떠올릴 경우에는 사생활의 보호는 근거로서 충분하지 않다.[108]

개인정보의 보호를 통해 부수적 또는 간접적으로는 재산에 대한 침해를 방지할 수도 있고, 그 외에도 개인이 갖는 구체적인 법익을 보호하는 수단이 될 수 있겠으나 근본적으로 개인정보자기결정권은 상기와 같이 개인의 인격을 보호하기 위한 권리로 이해된다. 이와 같이 볼 때, 인격권을 근거로 하는 개인정보자기결정권 자체에서 적극적이고 개별적인 통제권의 근거가 도출된다고 보기는 어렵다. 인격의 침해 가능성은 타인에 의해 개인정보가 활용되었다는 사실 자체로부터 발생하는 것이 아니라 정보주체가 알거나 예상하지 못했던, 그리하여 통제권 행사의 기회를 적절히 부여받지 못한 신상정보의 이용과 개인정보의 오남용에서 발생하며, 개인정보자기결정권으로부터 도출되는 통제 권능은 그와 같은 침해 가능성을 방지하기 위한 최소한의 장치를 개인에게 보장하는 것이기 때문이다. 정보주체가 자신의 편익을 위해 개인정보를 적극적으로 제공 및 활용하고, 또한 타인의 변형된 개인정보로부터 편익을 얻으며 살아가는 현대 사회에서의 개인정보자기결정권의 내용은, 정보주체가 정보처리여부를 개별적으로 통제할 수 있는 권리라기보다는 정보의 유통에 대해서 통제하고 참여할 수 있는 권리로 보는 것이 타당하다.[109]

---

108) 개인정보자기결정권은 개인정보자기결정권은 사회로부터 은둔할 수 있는 사생활 영역의 권리가 아니고, 사회에 참여하는 데 필요한 사회적 영역의 권리이기 때문에 헌법 제17조를 그 근거로 볼 수 없다는 지적에 대해서는 프라이버시 정책연구 포럼, 개인정보 보호법제 개선을 위한 정책연구보고서 (2013), 8 참조.

109) 이희옥, “개인정보 자기결정권에 관한 비판적 검토”, 법제 통권 제675호 (2016), 30.

만일 개인정보자기결정권의 보장 수단을 입법화한 법령 규정 또는 그에 대한 해석이, 개인의 적극적인 권능의 범위를 응당 개인에게 보장되어야 할 통제 권능과는 관련성이 낮은 범위까지 확장한 결과 제3자의 법익이 침해될 가능성을 초래한다면, 이는 개인정보자기결정권의 보장범위를 잘못 이해한 과도한 입법 또는 해석일 수 있다. 독일의 연방헌법재판소는 1983년의 인구조사판결을 통해 개인정보 자기결정권을 헌법상 권리로 인정하면서도, 정보에 대한 자기결정의 권리는 무제한이 아니고 절대적 통제라는 의미의 권리를 갖지 않는다는 점, 오히려 개인은 개인은 사회공동체 내에서 전개되고 의사소통하는 인격체이므로, 개인적인 정보일지라도 해당 개인에게 배타적으로 귀속될 수 없는 사회적 현실을 반영하는 것이라는 점, 고로 기본적으로 개인은 정보에 대한 자기결정권보다 우월한 공익에 의한 제한을 받아들여야 한다는 점을 분명히 설시하였다.[110] 개인정보 보호 법령상 개인정보의 이용을 제한하는 취지의 규정들을 해석함에 있어서는, 개인에게 부여되는 통제권이 합당한 범위를 벗어나 필요 이상으로 확장되지 않도록 하는 비판적 검토도 필요하다고 할 것이다.

---

110) BverfGE 65, 1 ff.
"Dieses Recht auf "informationelle Selbstbestimmung" ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über BVerfGE 65, 1 (43)BVerfGE 65, 1 (44)"seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden (BVerfGE 4, 7 [15]; 8, 274 [329]; 27, 1 [7]; 27, 344 [351f]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen."

제 2 절 개인정보 관련 규제별 적용범위의 차등화

1. 정보통신망법상 개인정보 관련 규율

정보통신망법은 제4장에서 “개인정보의 보호”라는 표제 아래 개인정보에 관한 규율을 정하고 있다. 가장 먼저 등장하는 조문인 제22조(개인정보의 수집 이용 동의 등)를 보더라도, 개인정보를 수집 및 이용하기 위하여서는 원칙적으로 수집 시에 일정한 사항을 이용자에게 알리고 동의를 얻을 것을 요구하고 일부 특단의 사정이 있는 경우에 한해 예외적으로 동의를 면제하고 있다. 개인정보의 수집 및 이용이 가능한 사유 중 하나로서 정보주체의 동의를 나열하면서 상대적으로 보다 폭넓게 동의 면제 사유를 인정하고 있는 개인정보 보호법 제15조에 비해 상대적으로 동의 기반의 활용 원칙에 보다 중점을 두며 강화된 규율을 가지고 있다는 점을 알 수 있다.

이와 같은 강화된 규율은 개인정보의 생애주기 전반에 걸친 각 단계별 규제에서 마찬가지로 반복된다. 정보통신망법상의 주요 의무 유형으로는 개인정보 처리에 대한 동의제도 이외에도 개인정보처리방침 작성 및 개인정보 보호책임자 지정 의무, 이용자의 열람·제공 요구권, 이용내역 통지의무, 파기의무, 기술적 관리적 조치의무, 유출사고 발생 시의 통지 및 신고 등의 대응의무 등이 있다. 가장 명확히 대조 가능한 사항으로서, 이용내역 통지의무(제30조의2)나 흔히 개인정보 유효기간제로 별칭되는 장기 미이용자 개인정보에 대한 파기 등 조치의무(제29조 제2항)는 정보통신망법에만 존재한다. 관련하여 선행 연구중에서는 EU와 일본의 개인정보 보호 법령, 개인정보 보호법과 정보통신망법상의 규제 수준을 비교하면서 규제의 강도를 정량적으로 수치화하는 연구 방법을 사용한 사례가 있는데, 해당 연구에 따르면 GDPR을 기준으로 일본 개인정보 보호법은 1.4배의 규제가 더 있는 셈이고, 개인정보 보호법은 2.6배, 정보통신망법

은 3.4배의 규제가 더 존재한다고 한다.[111]

사업자에게 부과되는 개별적인 의무들이 근본적으로 어떠한 취지를 갖는지에 대해서는 개인정보 보호법 제4조를 참고할 수 있을 것으로 보인다.[112] 동조는 정보주체가 갖는 개인정보에 대한 기본적인 권리 내용을 유형화하고 있는데, 정보통신망법상의 구체적인 규제 내용들을 일대일로 대응시키기는 어렵더라도, 어떠한 권리를 보호하기 위한 것인지 취지를 이해하고 유형화하는 데에 참조할 수 있을 것으로 생각된다.

<표 4-1> 정보주체의 권리에 대응하는 사업자의 의무

개인정보의 처리에 관한 정보를 제공받을 권리	• 동의 수집 시의 고지사항 • 개인정보처리방침 수립 및 공개의무
개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리	• 개인정보 처리 시의 동의 획득 의무 (동의 수집 시의 고지사항, 처리 내용별로 구분하여 동의를 얻을 의무)
개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람 요구할 권리	• 이용내역 통지의무 • 열람·제공요구에 응할 의무
개인정보의 처리 정지, 정정·삭	• 정정 및 동의 철회권

111) 김경환, “규제 측면에서의 한국 EU 일본의 개인정보 보호 법령의 비교”, 2017 Naver Privacy White Paper(2017), 35.

112) 개인정보 보호법 제4조

> 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.
> 1. 개인정보의 처리에 관한 정보를 제공받을 권리
> 2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
> 3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
> 4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
> 5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

제 및 파기를 요구할 권리	• 파기 및 분리보관의무
개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리	• 개인정보 유출 등의 통지 신고의무 • 손해배상 및 손해배상의 보장 의무113)

2. 합리적인 해석의 기준

앞서 반복하여 언급한 것과 같이, 정보통신망법상의 규제 범위는 개인정보자기결정권의 합당한 내용과 사업자의 영업의 자유 사이의 조화로운 균형이 이루어질 수 있도록 합리적으로 설정되어야 한다. 그리고 이와 같은 합리적인 범위 설정의 문제는 1차적으로는 입법에 맡겨야 할 문제이나, 법령의 불가피한 추상성에 따라 해석의 영역에 맡겨질 수도 있다.

본장에서는 이론상 개인을 식별할 가능성이 있는 모든 정보에 대해 동일한 수준으로 적용 가능하도록 규율된 입법 형식과 개인정보의 보호에 치우친 규제 적용 기조를 주된 원인으로 하여, 사업자에게 과중한 부담으로 작용하고 있는 정보통신망법상의 개별 규제에 대해 합리적인 해석의 범위를 도출하여 볼 것이다. 동일한 '개인정보'라고 하더라도 규제 유형별로 그 범위를 차등해석하여야 할 필요성이 있다는 지점에서 출발하여, 개별 의무 규정의 적용 여부 내지는 적용의 효과에 있어서 차등화를 꾀할 수 있는 방안과 그 근거를 고안하였다.

이와 같은 차등화된 해석이 논리적인 일관성을 갖기 위해서는, 개인정보자기결정권과 영업의 자유가 충돌하는 각 규제별로 합리적인 이익형량이 담보되도록 하는 전체적인 방향성 내지는 기준이 필요하다. 이를 위하여는 분석 대상인 개인정보 관련 규제별로 개인정보자기결정권의 보호 필요성이 가장 긴절한 것은 무엇이고, 반대로 영업의 자유에 무게를 두어야 할 필요성이 높은 것은 무엇인지 분석하여 보는 시도가 의미를 가질 수 있다. 이에 대해서는 물론 다양

113) 2019. 6. 13.부터 시행되는 개정 정보통신망법에 신설되는 제32조의 3(손해배상의 보장) 참조.

한 견해가 제시될 수 있으며, 하나의 규제 유형 안에서도 구체적인 요건과 개인정보 처리 맥락에 따라 서로 다른 지점에서 균형점이 형성될 수 있다. 예컨대 동일한 동의 획득 의무라고 하더라도, 개인정보 수집 및 이용에 대한 동의와 제공에 대한 동의는 개인정보 보호 필요성 수준이 서로 상이할 수 있다. 그러나 개인정보 범위의 차등해석에 관한 논의는 규제의 취지와 성격에 따라 규제 필요성 수준을 객관적으로 규명하여 보는 것에서 출발하여야 하므로, 본 연구서에서 논하고자 하는 대표적인 개인정보 관련 규제 별로 풀이하여 보았다.

먼저 개인정보에 대한 보호조치의 경우, 일응 개인정보자기결정권의 보호필요성이 가장 높은 수준으로 요구되며, 그에 따라 규제의 대상이 되는 정보의 범위도 가장 넓을 것으로 생각된다. 이에 대해서는 다음과 같은 근거를 제시해 볼 수 있다. 이용자의 개인정보를 어떠한 근거에 의하여든 입수하게 된 사업자는 이용관계, 즉 당사자간의 민사적인 계약관계 또는 신의칙에서 유래하는 부수적 주의의무에 의하여서라도 해당 정보를 보호할 의무를 부담한다. 사업자가 필요에 의해 또는 수집 및 보유하는 타인의 개인정보가 제3자에게 함부로 유출되지 않도록 기술적 관리적 보호조치 등을 하여야 할 의무는, 법령상 그러한 의무가 구체적으로 설정되기 이전에라도 이미 조리 등에 따라 사업자가 응당 부담하여야 할 의무이다. 사업자가 필요한 보호조치를 취할 경우 개인정보 유출 사고 등으로 인한 사업자의 책임 또는 위험 역시 감소될 수 있으므로, 구체적인 의무 수준을 어떻게 설정하는지와는 별개로, 의무의 성격만을 볼 때, 보호조치의무는 사적 자치나 영업의 자유에 대한 제한의 정도가 약하다. 또한 이용자의 입장에서도, 필요한 조치가 제대로 이루어지지 않을 경우 그 순간 이용자의 개인정보가 의도하지 않은 제3자 내지는 공개된 장소에 바로 노출될 수 있으므로, 개인정보자기결정권의 발현이 가장 긴절하게 요구되는 사항이라고 할 수 있다.

그 다음은 이용자의 개인정보 처리에 대해 동의를 얻을 의무이다. 개인정보자기결정권의 보장을 위하여 생래적으로 ‘동의’가 반드시 필요하다는 것은

아니다. 정당화의 근거가 무엇이든지간에 적법한 처리근거를 보유한 사업자만이 이용자의 개인정보를 처리할 수 있고 우리 법에서는 그 근거가 동의를 중심으로 설정되어 있기 때문에 동의가 주요하게 요구되는 것이다. 이러한 취지에서 동의의 획득은 적법한 처리 근거에 대한 사업자의 가장 적극적인 입증활동이기도 하다. 이 때문에 "동의 획득"은 보다 엄밀하게는 "적법한 처리근거의 요구 및 확인"을 의미한다고도 할 수 있다. 동의 획득 요건을 통해, 이용자로서는 자신의 개인정보가 본인의 의도와 상관 없이 제3자에게 입수되지 않는다는 보장을 확보하게 되며, 법리상으로는 동의의 범위 내에서 개인정보의 침해에 대한 일종의 양해가 이루어지게 된다.[114] 이러한 장치가 없을 경우 개인정보는 이용자의 의사나 정당한 처리 목적과 상관 없이 확산되는 등 매우 쉽게 위험상태에 놓일 수 있다는 점과, 홈페이지 내지는 어플리케이션을 통해 이용자와 지속적으로 접촉하며 서비스를 제공하는 정보통신서비스의 경우 이용자로부터 동의를 얻는 절차가 사업자에게도 추가적으로 큰 부담이 되지 않는다는 점에서 영업의 자유보다는 개인정보자기결정권에 무게를 둘 수 있을 것으로 생각된다.[115]

그 외에 사업자에게 부과된 의무들은 개인정보자기결정권의 본질에서 보다 벗어나 있거나, 행정적 목적을 위하여 작위의무를 새로이 부과하는 측면이 조금씩 강화된다. 개인정보가 유출되었을 때 제3자에게 발생한 손해를 배상하고 사고의 결과를 복구하는 것은 책임 있는 당사자가 당연히 이행하여야 할 의무이나, 일정한 기간 이내에 정부 부처에 서식을 갖추어 신고를 하거나 개별 이

114) 동의의 예외사유에 해당하는 경우는, 계약 이행 등을 위해 이용자의 묵시적 동의의사가 인정된다거나, 또는 법령상 요구되는 개인정보 처리로서 이용자의 의사와는 당초부터 무관한 것으로 설명할 수 있다.

115) 개인정보 관련 규제가 형식화된 동의 만능주의로 흐를 경우, 동의의사를 실질적으로 확보하였는가 내지는 이를 입증할 수 있는가가 아니라 매 서비스 제공 국면마다 형식상 완벽한 동의절차를 구현해두었는지 등을 의무 이행 여부의 척도로 하는 데서 오는 사업자의 부담과 비경제에 대해서는 별론으로 한다.

용자 모두에게 통지를 마쳐야 한다는 것은 불법행위의 책임으로부터 바로 도출되지 않는다.

개인정보의 파기의무의 경우, 행정안전부의 개인정보보호법령 및 지침 고시 해설 자료에서는 그 취지에 대해 “개인정보를 수집한 목적이 달성된 경우에도 계속해서 보유할 경우 개인정보의 유출과 오용 가능성이 높아지므로 더 이상 개인정보가 불필요하게 된 때에는 이를 파기하도록 함으로써 개인정보를 안전하게 보호하려는 것”이라고 설명한다.[116] 개인정보의 유출과 오용에 대한 직접적인 방지 수단으로서 보호조치의무를 부과하면서, 일정 기간 이후로는 아예 유출 등 침해사고의 여지가 차단되도록 개인정보를 장기간 보유하지 못하게 하는 이중의 장치를 마련한 것이다. 사인이 적법한 근거에 의해 보유하는 자산에 대해 보유 목적이 달성되었다거나 더 이상 필요하지 않다는 이유로 파기의무를 부과하는 입법례는 찾아보기 힘들다. 설령 이용자가 동의 등을 통해 사업자에게 적법한 보유 권한을 부여했다고 하더라도 소유재산을 처분하는 것과 같이 개인정보에 관한 권리를 포기하는 것은 아니라는 시각에 기반한 것으로 이해되며, 현행 법령상 이용자는 사업자가 명시한 보유 및 이용기간을 확인하고 그에 대해 동의를 한다는 점, 인격권에서 유래하는 개인정보자기결정권은 일신전속적 성질을 갖는다는 점 등에 비추어 볼 때 취지 자체에는 수긍할 수 있다.

그러나 사업자가 개인정보를 계속하여 보유한다는 것만으로 이용자에게 어떠한 피해가 발생하지는 않는 반면, 파기의무를 부담하는 사업자로서는 사업에 관한 정보자산으로서 재산적 가치가 있는 정보들을 개인정보로서 파기하여야 한다거나, 목적 달성이라는 불명확한 요건에 좌우되는 파기의무를 부담하면서 구체적인 피해를 발생시키지 않고서도 의무를 미이행한 것만으로 형사처벌을 받을 수 있다는 점[117] 등을 볼 때, 사업자의 영업의 자유에 대한 제한 측면이

116) 행정안전부 등, 위의 책, 120.
117) 정보통신망법 제73조 제1의2호

더욱 더 비중있게 고려될 필요가 있다.

나아가 열람·제공과 이용내역 통지의 경우 개인정보 처리 내역에 대한 정보를 제공한다는 취지만을 본다면, 개인정보자기결정권 행사의 전제로서 핵심적인 보호 수단에 해당할 수 있다. 다만 법은 이미 일반적인 개인정보 처리 현황을 개인정보 처리방침을 통해 공개하도록 하고 있을 뿐만 아니라, 사업자가 열람·제공과 이용내역 통지를 통해 알려야 하는 개인정보 처리 내역은 법령상 전혀 구체화되어 있지 않고, 합리적으로 경계가 설정되어 있다고도 보기 어렵다. 예컨대 이용자가 정보통신망법 제30조 제2항 제2호에 근거하여 정보통신서비스 제공자에게 '본인의 개인정보를 이용한 현황'을 제공해 줄 것을 요구할 경우, 과연 어느 정도 구체적인 이용 내역까지 알려야 하는지 명확치 않으며 이에 대한 판단과 미이행으로 인한 책임은 오로지 사업자에게 맡겨져 있다. 더구나 요청이 있을 경우에 한해 응답하여야 하는 열람제공요구권과는 달리 이용내역 통지제도의 경우 일정 규모 이상의 정보통신서비스 제공자에게 전체 이용자에 대하여 주기적으로 통지를 이행하도록 하는 것으로서 사업자의 부담은 더욱 클 수밖에 없다.

아래에서는 적용 범위에 관하여 논란이 계속되고 있는 열람제공요구권 및 이용내역통지 제도를 중점으로 하여 합리적인 해석방안을 고안해 보고자 한다. 또한, 효율적인 논의를 위하여 앞서 정리한 개인정보의 유형별 분류 중 개인정보에 해당하는지 여부가 현재 명확히 정리되지 않은 '개인식별정보와 결합되지 않은 상태의 개인식별가능정보' 등을 중심으로 대상을 좁혀 검토하였다.

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
1의2. 제29조 제1항을 위반하여 개인정보를 파기하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

제 3 절 정보통신망법상의 각 의무별 합리적인 해석방안

1. 이용자의 열람제공요구권 행사에 대한 조치의무

<표 4-2> 이용자의 열람제공요구권 관련 규정

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조(이용자의 권리 등) ② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다. 1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보 2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황 3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황 ④ 정보통신서비스 제공자등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.

사업자가 보유하는 개인정보 항목과 이용 및 제3자 제공 현황 등을 알리도록 하는 이용자 열람제공요구권의 경우, 앞서 지적한 것과 같이 개인정보 개념에 더하여 행위의무의 내용마저 불분명하게 규정된 측면이 있다. 이로 인하여, 법령의 해석에 있어 열람 및 제공의 대상인 개인정보의 범위를 무한정 확장하는 경우 사업자에게 많은 노력과 비용을 소모할 것을 강요하는 것이 될 뿐 아니라, 사실상 이행이 불가능한 의무를 강요하는 결과가 될 수 있다.

이용자 열람제공요구권이 알 권리 보장 측면에서도 그 자체로서도 이용자의 권리를 보호하는 측면을 가진다는 것은 분명하나, 정보의 처리 현황을 아는 것만으로는 개인정보의 보호라는 결과를 달성할 수 없다. 결국 이용자가 구체적으로 정정 요구 내지는 동의 철회 등의 적극적인 권리를 행사할 수 있도록 하기 위한 전제 조건으로서의 성격이 강하다고 할 것이다.[118] 따라서 이용자 열

람제공요구권의 대상이 되는 개인정보의 범위를 검토함에 있어서는, 이용자가 스스로 개인정보 자기결정권을 행사하기 위하여 충분한 정보를 파악할 수 있도록 하는 것이 취지이며, 이와 같은 권리 행사와는 실질적인 관련성이 없는 정보에 대해서까지 열람제공요구의 대상이 된다고 보는 것은 수범자에게 불필요한 부담을 가중할 수 있다는 점이 고려되어야 한다.

가. 개인식별정보와 결합되지 않은 상태의 개인식별가능정보

개인식별정보 또는 개인식별정보와 결합되어 있는 개인식별가능정보의 경우에는 개인정보로서 이용자 열람권의 대상이 된다는 점, 반대로 개인을 식별할 수 없는 정보의 경우에는 열람제공요구의 대상이 될 수 없다는 점이 비교적 명확하다. 문제는 "개인식별정보와 결합되지 않은 상태의 개인식별가능정보"가 열람제공요구의 대상이 되는지 여부이다.

먼저 1인으로 귀속되는 정보[119]에 해당하여 신원을 알 수 없는 특정한 1인으로 정보들을 귀속시킬 수 있을 정도로만 식별가능성이 유지되어 있는 경우, 추가적인 결합 등의 조치를 함으로써 정보의 보관 상태를 변경하지 않는 한 사업자로서도 이미 해당 정보만으로는 개인이 누구인지를 특정할 수 없게 된다. 예컨대 다양한 행태정보가 광고식별자와 같은 고유값이 부여된 상태로 개별적인 목적에 따라 수집되어 분산된 형태로 저장되어 있을 수 있다. 이 때, 정보통신서비스 제공자조차도 각각의 행태정보가 어느 이용자에게 귀속되는지 확인하기

---

118) 권영준, "개인정보 자기결정권과 동의 제도에 관한 고찰", 2015 Naver Privacy White Paper(2015), 100.
"개인정보의 처리를 확인하고 개인정보에 대하여 열람을 요구할 권리는 한편으로 는 개인정보의 사전적 동의권의 실효성을 높이고, 다른 한편으로는 개인정보의 사후적 통제권 행사를 용이하게 하여 주는 보조적 권리이다. (중략) 따라서 이는 개인정보 자기결정권의 사전적 또는 사후적 행사를 지원하여 주는 법적 도구라고 볼 수 있다."

119) 본 연구서 51면 참조

위하여서는, 별도로 보유하고 있는 개인식별정보와 결합된 광고식별자 정보를 추가로 확인하여야 하며, 이를 특정 이용자 1인에 대한 정보 보유 내역과 같은 형태로 완성하기 위하여서는 개별 행태정보 모두에 대해 위와 같은 작업을 거쳐야 한다. 이와 같은 1인으로 귀속되는 정보의 경우에는, 그 중 어떤 정보가 이용자가 열람제공요구권을 행사한 이용자에 대한 정보인지 구별할 수 없으므로 열람제공의 대상에서 제외되어야 한다고 봄이 타당하다.

이에 대하여는 이론적인 식별가능성이 존재하는 이상, 사업자가 개인을 식별하기 위한 조치를 거쳐 개인정보 처리 현황 일체를 파악하여 이용자에게 제공해야 한다는 이론이 있을 수 있다. 그러나 이는 개인정보를 보호하고자 하는 목적으로 개인식별정보와 별도의 서버에 보관하면서 엄격하게 관리·통제하여 온 정보를 이용자의 열람·제공 요청에 따라 개인식별정보와 연결해야 한다는 것으로서, 사업자에게 불필요한 인력과 비용의 투자를 강요하는 것이 될 뿐 아니라, 오히려 이용자의 개인정보 침해의 위험성을 증가시키게 되어 이용자의 요청의 취지에도 부합하지 않으며 개인정보 보호 제도의 취지 및 최소수집 원칙에도 역행하는 것이 된다.

이러한 사정은 특정한 1인으로 귀속시키는 것조차 어렵도록 흩어져 있는 정보의 경우에도 동일하게 적용된다. 예를 들어, SNS 서비스에 업로드된 사진·영상 등의 컨텐츠에 대해 이용자가 자신이 등장하는 화면은 개인정보에 해당하니 이를 모두 파악하여 정리해줄 것을 요구하는 경우가 있을 수 있다. 만약 이와 같은 요청에 대해서도 사진이나 영상이 개인정보라는 이유만으로 SNS에 업로드된 모든 사진·영상 중 해당 이용자가 등장한 부분을 찾아 전달해주어야 한다면, 사업자에게 과도한 부담을 지우는 부당한 결과를 발생시키게 된다. 향후 각종 온라인 서비스의 발달로 인하여 이용자에 관한 각종 정보가 수집 및 축적될 것을 고려하면 정보 제공 현황 파악에 대한 이용자의 니즈는 더욱 커질 수 있다. 사업자가 당초부터 이용자를 식별하여 정보를 처리할 의사를 갖고 있지 않았으며, 그로 인하여 개인식별정보와도 완전히 분리된 상태로 보관되어

있는 정보는 열람제공요구권의 대상에서 제외된다는 명확한 해석이 필요하다고 본다.[120]

GDPR 제11조[121] 또한 개인정보처리자가 그 정보처리 과정에서 개인의 식별을 필요로 하지 않는 경우에는 동법을 준수하기 위한 목적에서 개인을 식별하기 위해 추가적인 정보 처리를 거칠 의무는 없으며, 과거에 정보 처리 목적으로 식별을 필요로 하였던 정보라 하더라도 '더 이상(no longer)' 식별정보가 아닌 상태에 있다면 사업자가 열람 제공을 위하여 재식별화 처리를 할 필요는 없다는 기본 원칙을 제시하고 있다.

또한 일본의 개인정보의 보호에 관한 법률에도 정보통신망법상의 열람제공요구권과 유사한 이용자의 개시청구권이 규정되어 있는데, 일본의 경우 법령에서 직접적으로 개시의 대상을 개인정보가 아닌 "당해 본인이 식별되는" 보유개인데이터라고 한정적으로 정하면서 익명가공정보를 열람 대상에서 명시적으로 제외하고 있다. 또한 '보유개인데이터'라는 개념은 개인정보와는 구별되는

120) 다만 이와 같은 사례들은 규제의 적용범위에 대한 해석론을 통하지 않고도 개인정보성 단계에서 해석상 배제하는 것 역시 가능하다. 언급한 사례와 같은 경우는 결합에 수반되는 비용이나 노력이 합리적인 수준을 넘으므로 개인정보에 해당하지 않는다거나, 개인정보 보호법상의 개념이기는 하나 개인정보처리자가 개인정보파일 형태로 보관하는 정보가 아니라는 이유로 열람제공요구의 대상이 아니라는 논리 전개 및 결론도 가능할 것으로 보인다.

121) GDPR 제11조 (개인정보보호위원회 번역문)

> 제11조 신원확인을 요하지 않는 개인정보의 처리
> 1. 개인정보처리자가 개인정보를 처리하는 목적상 개인정보주체의 신원확인을 요구하지 않거나 더 이상 요구하지 않아도 되는 경우, 그 개인정보처리자는 본 규정을 준수할 목적에 한하여 개인정보주체를 식별하기 위한 추가 정보를 유지, 취득, 처리할 의무를 가지지 않는다.
> 2. 본 조 제1항에 규정된 사례의 경우 개인정보처리자가 개인정보주체를 식별할 수 없음을 입증할 수 있다면, 제15조부터 제20조까지의 조문은 적용되지 않는다. 단, 개인정보주체가 해당 조문에 따라 본인의 권리를 행사하기 위한 목적으로 본인의 신원을 확인할 수 있는 추가 정보를 제공하는 경우는 예외로 한다.

것으로, “개인정보데이터베이스” 및 “개인데이터”의 정의에 비추어 볼 때, 개인정보처리자가 직접 운영하는 개인정보를 검색할 수 있는 시스템에서 검색을 통해 추출 가능한 정보를 전제로 한다. 일본법은 개시청구의 대상을 ‘보유개인데이터’라고 정함으로써, 데이터베이스에 저장되어 있지 아니한 개인정보 또는 수탁자를 통해 처리하는 개인정보를 제외하고 있어 개시 대상이 무한정 확장될 우려가 상대적으로 덜하다. 이와 관련하여, 일본 개인정보보호위원회는 Q&A 자료를 통해 ‘사내에서 취급하는 개인정보가 특정의 개인정보를 검색할 수 없는 상태로 보관되어 있다면 개인정보에 해당하지 않아 개시의무의 대상이 되지 않는다’는 입장을 밝히고 있다.[122]

<표 4-3> 일본 개인정보의 보호에 관한 법률의 개시청구권 관련 규정

제28조(개시) ① 본인은, 개인정보취급사업자에 대하여 당**해 본인이 식별되는 보유개인데이터의 개시**를 청구할 수 있다. ②개인정보취급사업자는 전항의 규정에 의한 청구를 받은 때에는, 본인에 대하여 政令으로 정하는 방법에 따라 지체 없이 당해 보유개인데이터를 개시하여야 한다. 다만, **개시함으로써 다음 각 호 중 어느 하나에 해당하는 경우에는 그 전부 또는 일부를 개시하지 않을 수 있다.** 1. 본인 또는 제3자의 생명, 신체, 재산 기타의 권리이익을 해할 우려가 있는 경우 2. 당해 개인정보취급사업자의 업무의 적정한 실시에 현저한 지장을 줄 우려가 있는 경우 3. 다른 법령에 위반하는 것이 되는 경우 제2조(정의) ① 이 법률에서 “**개인정보**”라 함은 생존하는 개인에 관한 정보로서, 다음 각 호의 어느 하나에 해당하는 것을 말한다. (중략) ④ 이 법률에서 “**개인정보데이터베이스 등**”이라 함은 개인정보를 포함하는 정보의 다음에 열거된 것(이용방법으로 보아 개인의 권리이익을 해할 우려가 적은 것으로서 정령으로 정하는 것을 제외한다)을 말한다.

122) 日本 個人情報保護委員会, 「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ(2017), 41.

1. 특정의 개인정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것
2. 전호의 것 이외에, 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로서 정령으로 정하는 것
⑥ 이 법률에서 "**개인데이터**"라 함은 개인정보데이터베이스등을 구성하는 개인정보를 말한다.
⑦ 이 법률에서 "**보유개인데이터**"라 함은 개인정보취급사업자가 개시, 내용의 정정·추가·삭제, 이용의 정지, 삭제 및 제3자제공의 정지를 행할 수 있는 권한을 가지는 개인데이터로서, 그 존부가 밝혀짐에 따라 공익 기타의 이익이 침해될 수 있는 것으로서 정령으로 정하는 것 또는 1년 이내에서 정령으로 정하는 기간 내에 삭제하게 되어 있는 것 이외의 것을 말한다.

나. 내부적 목적으로만 이용되는 사업자 생성정보

한편 사업자가 스스로 생성한 정보가 사업자 이외의 제3자에게 제공되지 않고 내부적인 관리상의 목적 또는 이용자에 대한 서비스 제공의 목적으로만 이용되는데 그친다면, 해당 정보는 사업자의 지배 영역에서만 생성되고 이용되는 정보로서 이용자의 열람제공요구권의 범위에서 제외될 수 있다. 그러한 정보가 생성된다는 사실은 서비스 이용 과정에서 당연히 예상 가능한 것일뿐더러, 사업자가 해당 개인과 직접적인 관련 없이 업무처리만을 위한 목적으로 생성한 정보[123]마저도 개인정보에 해당한다고 보아 보유 현황과 처리내역을 이용자에게 제공하여야 한다면, 사업자의 내부적인 정보를 불필요하게 노출하도록 강요하는 것으로서 영업의 자유를 과도하게 제한하는 결과가 될 수 있다. 반면에 이용자 입장에서는 그와 같은 정보를 확인하지 못한다고 하더라도 개인정보자기결정권을 제한당한 것이라고 보기 어렵다. 특히 열람제공요구권은 정보의 보유 여부와 내용 등을 확인하고 정보 정정 또는 동의 철회 등으로 나아가기 위한 사전적인 권리행사 수단이라는 점과 이용자로서는 사업자가 내부적 목적으로 보유 및 이용하는 정보에 대해 내용의 정정을 요청하거나, 다른 정보는 그

123) 예컨대 온라인 쇼핑몰을 운영하는 사업자가 각 주문마다 일련번호를 부여하여 관리하는 경우가 이에 해당한다.

대로 두면서 이에 대하여만 별도로 동의를 철회할 실익이 없다는 점에서 더욱 그렇다.

또한 사업자가 생성한 정보의 경우 사업자의 영업비밀과 직결된 정보가 있을 수 있어, 이러한 정보들을 이용자 열람요구제공권 행사에 의해 외부에 유출할 것을 법적으로 강제하는 것은 부당하다.[124] 예컨대 AI 관련 서비스 제공 과정에서 이용자를 식별하기 위해 이용자의 여러 음성을 분석한 음성분석파일의 경우, 사업자가 서비스 제공을 위해 내부 이용 목적으로 생성한 파일로서, 만약 이러한 분석파일 생성을 위해 사업자의 특수한 기술이 이용되었다면 해당 음성정보파일을 이용자에게 제공함으로써 사업자의 영업 비밀이 침해될 우려도 있으며, 새로운 유형의 맞춤형 서비스의 경우 사업자가 특정한 정보를 기록하며 관리 및 활용한다는 사실 자체가 영업비밀에 준하는 것일 수 있다.[125]

이용자에게 보장된 개인정보자기결정권이 자신의 개인정보가 유통되는 모든 과정에 대해 참견하고 결정할 수 있는 권한을 부여하는 것은 아니라는 점은 앞에서 살펴본 바와 같다. 열람제공요구권 역시, 이용자가 권리를 행사하여 얻은 정보를 기초로 사업자에게 자신의 개인정보를 어떻게 사용할지에 대해 지시하고 간섭할 수 있도록 하기 위한 권리가 아니므로, 사업자가 서비스 이용기록을 서비스 제공 내지는 개선 등을 위한 목적으로 활용한다는 것을 알리는 것으로 족할 것으로 생각된다. 그와 달리 사업자가 자발적으로 서비스를 이용하는 이용자에 대해 관리 내지는 관찰한 결과를 외부와 공유하지 않고 이용하는 것에

---

124) 정보통신망법에는 일본 개인정보의 보호에 관한 법률 제28조 2항과 같이 이용자의 열람제공요구에 거부할 수 있는 예외사유에 대한 규정도 마련되어 있지 않다.

125) “분석데이터는 정보주체의 동의를 받아 수집된 정보를 기초하여 그에 대한 분석 정보이므로, 이에 대한 정보주체의 소유권귀속 문제에 대해서도 생각해 보아야 할 것이다. 상황에 따라서는 이를 영업비밀의 범위로 보아 개인정보 처리자의 독립된 생산물로 판단할 수 있는 여지도 있을 수” 있다고 지적하며 관련 제도의 공백을 지적한 연구로는 고유홈, “빅데이터와 개인정보보호”, 이슈와 동향 21권(2014), 71 참조.

대하여, 구체적이고 지엽적인 이용 목적과 방법에 대해서까지 이용자에게 알려야 한다는 논리는 열람제공요구권의 목적과 취지상으로도 도출되지 않는다.

또한 이용자로서는 서비스 이용관계를 종료하거나 동의를 철회함으로써 자신과 관련된 개인정보를 파기하도록 할 수 있으므로, 열람제공요구권이 인정되지 않더라도 해당 개인정보에 대해 여전히 개인정보자기결정권을 행사할 수 있으며, 동일한 개인정보를 외부에 제공하여 위험을 발생시키는 경우에는 당연히 열람제공요구권이나 다른 통제권한의 범위에 포함된다. 이와 같이 보는 이상, 내부적 목적으로만 이용되는 생성정보를 열람제공요구권의 대상 범위에서 제외한다고 하여 개인정보 자기결정권이 실질적으로 침해될 우려는 없을 것으로 보인다.

2. 이용내역 통지제도

<표 4-4> 이용내역 통지제도 관련 규정

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조의2(개인정보 이용내역의 통지) ① 정보통신서비스 제공자등으로서 대통령령으로 정하는 기준에 해당하는 자는 제22조 및 제23조제1항 단서에 따라 수집한 이용자 개인정보의 이용내역(제24조의2에 따른 제공 및 제25조에 따른 개인정보 처리위탁을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니하다. ② 제1항에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지 주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다. 동법 시행령 제17조(개인정보 이용내역의 통지) ② 법 제30조의2제1항에 따라 이용자에게 통지하여야 하는 정보의 종류는 다음 각 호와 같다. 1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목 2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다.

3. 법 제25조에 따른 개인정보 처리위탁을 받은 자 및 그 처리위탁을 하는 업무의 내용 ③ 법 제30조의2제1항에 따른 통지는 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 연 1회 이상 하여야 한다.

가. 이용내역 통지의 대상 범위

이용내역 통지제도는 정보통신서비스 제공자등으로 하여금 이용자의 개인정보 이용내역을 해당 이용자에게 주기적으로 통지하도록 함으로써, 이용자가 자신의 개인정보 이용내역을 정확히 알고 자기 정보를 통제할 수 있도록 하기 위하여 2013년 8월 시행된 개정 정보통신망법에 처음으로 도입된 제도이다.[126] 이메일 등을 통해 이용자에게 주기적으로 어떤 사업자가 자신의 정보를 어떻게 처리하고 있는지 현황을 알림으로써, 열람제공요구권에는 없는 환기 기능까지 더하여져 있어 동의의 철회, 정정 등 구체적인 권리의 행사를 더욱 적극적으로 장려하고 보장하는 기능을 하고 있다.

그런데 이용내역 통지의 경우, 의무주체가 매출액 또는 이용자가 일정 규모[127] 이상인 정보통신서비스 제공자에 한정되는 대신, 적극적으로 확인을 요청한 개별 이용자가 아니라 모든 이용자를 대상으로 일률적으로 통지를 행하여야 하며, 개인정보의 수집이용과 제3자 제공 내역 이외에 개인정보 처리위탁 내역 등까지 알려야 한다는 점에서 사업자의 부담이 더욱 크다. 특히 이용내역 통지제도는 한국의 고유한 제도라는 점에서 타국에서는 유사한 시스템을 구성하지 않고 있는 해외사업자에게는 보다 심각한 규제 부담으로 작용할 수 있다는 측면에서 적용 범위의 합리화가 더욱 강하게 요청된다.

---

126) 한국인터넷진흥원, 2012. 8. 개정 정보통신망법 개인정보보호 신규제도 안내서(2012), 5.

127) 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자를 가리킴(정보통신망법 시행령 제17조 제1항)

따라서 이용내역의 통지 범위에서도 열람제공요구권과 마찬가지로 개인식별정보와 결합되지 않은 개인식별가능정보와 내부적 목적으로만 이용되는 사업자 생성정보를 제외하는 것이 타당하다. 특히 전자와 관련하여서는, 전체 이용자를 대상으로 하는 이용내역 통지의 대상에 “개인식별정보와 결합되지 않은 상태의 개인식별가능정보”까지 포함되는 것으로 볼 경우, 1년마다 모든 이용자에 대하여 사업자가 가지고 있는 식별 가능성 있는 정보들을 전부 인위적으로 결합하여야 한다는 결론으로 이어지게 된다. 결과적으로 이용자에게 전달되는 내용은 법령상의 고지사항인 수집, 이용, 제공 및 처리위탁의 대상이 된 개인정보 항목과 목적, 개인정보를 제공 또는 처리위탁 받은 상대방 등에 대한 정보에 지나지 않음에도 불구하고, 사업자가 가지고 있는 개인식별가능정보를 모두 취합하여 특정 개인에게 연결함으로써 모든 정보의 식별가능성 수준을 개인식별정보의 수준으로 끌어올리게 되는 것이다. 이는 지나치게 비경제적일뿐 아니라, 모든 이용자를 대상으로 이루어진다는 점에서 개인정보의 침해 위험은 열람제공요구권과 비교하기 어려울 만큼 큰 문제가 될 수 있다.

한편 실무를 비롯한 일각에서는 이용내역 통지제도의 범위를 이용자로부터 수집된 개인정보에 한정하여야 한다는 의견도 제시되는 것으로 보인다. 사업자 생성정보에 대한 이용자의 통제권 행사 범위에 대해서는 사업자의 이익도 함께 고려하여 신중하게 접근할 필요가 있다는 점에서 문제 제기의 취지에 공감할 수 있다.

나. 통지 방법의 측면

이용내역 통지제도의 경우, 방법론적 측면에서도 합리화 방안에 대한 논의가 이루어질 필요가 있다. 구체적인 정보 제공 범위에 대하여 개별 이용자의 요청 취지에 맞추거나 이용자의 의사를 확인하여 조율하는 등의 방법으로 대처 가능한 열람제공요구권과는 달리, 이용내역 통지제도는 이용자 모두에게 일률적으로 전송되는 것이라는 특징이 있다. 실무상으로는 대부분의 사업자가 개인정보

처리방침의 내용을 사실상 그대로 전송함으로써 통지의무를 이행하고 있는 것으로 보이나, 방송통신위원회의 온라인 개인정보 처리 가이드라인은 이용내역의 통지 방법에 관하여 이용자별로 구체적 개별적인 내용으로 구성하여 맞춤형 통지가 될 수 있도록 노력하여야 한다고 언급하고 있다.[128] 이는 이용자의 권리를 보호할 수 있는 최선의 방안을 제시한 것으로서 바람직하다고 볼 수 있으나, 모든 사업자에게 이와 같은 구체적·개별적인 맞춤형 통지를 이행할 것을 기대하기는 어려울 것으로 보인다. 이용자의 개인정보 처리에 특히 신경을 쓰는 일부 대형 인터넷 기업의 경우, 이용자가 다양한 서비스에 걸친 개인정보의 처리 내역을 한 군데에서 함께 확인 및 관리할 수 있는 툴을 보유하고 있다. 그와 같은 개인화된 시스템 또는 기능을 활용하여서라면 가이드라인이 요구하는 이상적인 맞춤형 통지의 일부 취지를 실현할 수도 있을 것이나, 일반적인 정보통신서비스 제공자들은 그러한 통합 시스템을 갖추지 못한 경우가 더 많을 것으로 생각되는바, 모두에게 맞춤형에 이르는 수준의 조치를 요구하기는 힘들 것으로 생각된다. 이와 같은 환경에서 맞춤형 통지를 하도록 권장하는 동 가이드라인은, 이를 의무로서 요구하고 있다기 보다는 향후 이용내역 통지제도가 나아가야 할 바람직한 방향을 제시하고 있는 것으로 해석함이 타당해 보인다.

이용내역 통지제도의 도입 취지는 이용자가 자신이 가입한 웹사이트 또는 이용하고 있는 온라인 서비스 내역을 모두 기억하고 있지 못하거나, 수집한 개인정보의 이용 및 활용 내역을 정확히 알 수가 없어 더 이상의 이용이 불필요한 사이트에도 계속 가입된 상태를 유지함으로써, 불필요한 계정탈퇴, 패스워드 변경 등 이용자의 관리 노력을 기울이거나 권리를 행사함에 있어 현실적 제약이 존재한다는 점에 입각한 것으로 보인다.[129] 이용자가 인터넷 사이트 등의 가입내역을 모두 기억하지 못해 주의를 환기할 수 있도록 이용내역을 통지하도록

128) 방송통신위원회, 온라인 개인정보 처리 가이드라인(2011), 38.
129) 김정섭, “주민등록번호 없는 ‘클린 인터넷’ 환경 조성”, 통신연합 제61호(2012), 23.

하는 것은 일응 방법상으로 적절하다고 할 것이나 추가적으로 그 내용을 맞춤형 통지로까지 요구할 근거는 없는 것으로 보인다. 이용자에게는 정보통신망법에 따른 개인정보 열람제공요구권 행사라는 구체적인 권리 행사 수단이 마련되어 있고, 사업자는 개인정보처리방침을 별도로 수립 및 공개할 의무를 부담한다. 따라서 이용자로서는 개인정보처리방침을 통해 해당 사업자가 일반적으로 어떤 개인정보를 수집하고 어떻게 이용하는지를 알 수 있을 뿐 아니라, 그 중 자신의 개인정보 이용에 대한 보다 구체적인 내역을 알고자 하는 이용자라면 언제든지 열람제공요구권의 행사를 통해 파악이 가능하다. 이에 더하여 본래대로라면 이용자 스스로의 권리의식에 의해 해결하여야 할 개인정보 제공 사실에 대한 환기까지 사업자의 의무로 하는 것은, 간편한 이메일 발송으로 의무 이행이 가능한다는 전제에서는 합리화될 여지가 있다. 그러나 열람제공요구권 행사로서 충족될 수 있는 맞춤화된 정보 제공을 전 이용자에 대한 이용내역 통지에까지 반영할 것을 요구하는 것은 사업자의 업무상의 부담 내지는 의무 부과의 당위성을 고려하지 않은 과도한 제한으로 보인다.

3. 그 외의 규제에 대한 합리적인 해석 방안

가. 보호조치의무

개인정보의 분실이나 도난, 유출, 위조, 변조 또는 훼손을 방지하고 안정성을 확보하기 위한 법상의 보호조치의무[130]는 앞서 언급한 것과 같이 개인정보로서의 보호필요성이 가장 강한 수준으로 요구되는 규제 유형이라고 할 수 있다. 반면 사업자의 입장에서는 정보자산의 유출을 막는다는 스스로의 이익을 위하여서도 보안을 위한 조치를 할 유인이 충분하다.

---

130) 실정법상으로는 모법에 따라 행정안전부 고시인 개인정보의 안전성 확보조치 기준(개인정보 보호법)과 방송통신위원회 고시인 개인정보의 기술적·관리적 보호조치 기준(정보통신망법)를 통해 구체화되어 있다.

또한 법령상 의무적으로 요구되는 보호조치들은 대부분 정보처리시스템, 보안서버 등 개인정보가 처리되는 환경을 대상으로 하는 것이 대부분이어서 그 안에서 취급되는 개별 정보의 성격과 내용, 유형 등에 따라 요구되는 조치 수준을 달리 하여야 할 필요성이 크지 않다. 특히 구체적인 규정 중에서는, 조항 자체에서 개인정보의 내용과 유형에 따라 필요한 조치를 직접 차등화하고 있는 조항도 발견된다. 예컨대, 개인정보의 기술적·관리적 보호조치 기준[131] 제6조는 제1항에서 비밀번호의 경우 복호화 되지 아니하도록 일방향 암호화하여 저장해야 한다고 규정하면서도, 제2항에서 주민등록번호, 여권번호, 운전면허번호 등은 안전한 암호알고리듬으로 암호화하여 저장한다고 규정하여, 정보의 종류에 따라 조치 수준을 달리 정하고 있다.

이러한 점을 고려할 때, 앞서 분류한 것과 같이 식별가능성 또는 출처, 목적 등 개인정보의 내용을 기준으로 보호조치의 적용 여부를 달리 보는 것은 논리적 근거나 실익이 적을 것으로 보이므로 보호조치의무는 원칙적으로 모든 개인정보에 적용되는 것이 합당하다. 물론 보호조치의무 관련 개별 조항을 위반한 결과, 결합되지 않은 상태의 개인식별가능정보가 단독으로 유출되는 경우의 행정제재나 피해자에 대한 민사상의 책임 등과 같이 분쟁으로 발전하는 경우에는 해당 정보를 보호조치가 필요한 개인정보로 보느냐에 따라 사업자의 법익에도 미치는 영향이 작지 않을 것이다. 그러나 이는 개인정보 침해가 실제로 발생한 경우 사후적으로 고려할 요소라고 생각된다. 다시 말해 침해의 원인이 보호조치의무 위반에 있는지를 판단할 때 사안별로 문제가 된 정보의 내용, 처리의 목적과 방법, 침해의 결과 등 종합적인 사정을 평가할 때 식별가능성의 정도를 함께 고려할 수 있을 뿐, 사전적으로 개인정보를 유형화한 후 특정 유형 전체에 대해 보호조치를 배제하는 것은 적절하지 않을뿐더러, 실익도 마땅히 없을 것으로 생각된다.

나. 동의획득의무

131) 방송통신위원회고시 제2015-3호, 2015. 5. 19.

개인정보의 처리에 대하여 이용자로부터 동의를 얻을 의무는, 이른바 “informed consent”라는 개념 하에 고지의무와 맞물려 이용자에게 개인정보 처리 내역에 대한 정보를 투명하게 공개하고 1차적인 통제권을 보장하는 역할을 하며, 정보통신망법 및 개인정보 보호법에서 공히 개인정보 자기결정권을 보장하는 핵심적인 수단으로 기능하고 있다. 앞서 언급한 것과 같이 동의 절차를 통해 이용자는 자신의 개인정보가 자신이 모르는 사이에 개인정보가 처리되고, 오남용되지 않는다는 보장을 확보하게 된다는 점에서 의의가 있다.

그러나 현행 법령 및 규제 체제 하에서 동의제도는 통제수단으로서의 의의 내지 효용성을 지적받고 있다. 특히 동의원칙의 예외를 매우 좁게 인정하고 있는 정보통신망법의 경우, 개인정보 범위의 불명확성으로 인하여 발생할 수 있는 법 위반의 소지를 제거하기 위해 사업자들은 모든 정보를 일응 개인정보로 취급하여 이용자로부터 정보를 수집할 때마다 개인정보 처리에 대한 동의를 수집하고, 서비스를 이용하고자 하는 자는 개인정보에 관해 민감한 일부를 제외하고는 별다른 점검 없이 습관적으로 동의를 제공함으로써 실질적인 통제권으로서의 기능을 잃고 단지 면죄부로 기능하고 있다는 비판이 제기된다.[132]

이와 같은 문제점을 개선하기 위하여서는 다양한 방식의 접근이 필요하며, 특히 동의의 범위에 관하여서는 종국적으로는 개인정보의 종류 및 개인정보 처리의 단계별 위험성에 따라서 동의 방법을 구분하여 옵트 인과 옵트 아웃, 직접수집과 간접수집을 구별하여 요구하는 방안 등을 검토할 필요가 있다.[133] 사전 동의 원칙을 고수하고 관련 고지의무 등을 엄격하게 요구할수록 이용자에게 제시되는 동의의 숫자와 동의의 문구가 늘어날 수밖에 없고, 그 결과 동의라는 절차가 형식화되는 것이기 때문이다. 그러나 현행법 하에서 법개정 없이 해석

---

132) 권영준, “개인정보 자기결정권과 동의 제도에 관한 고찰”, 2015 Naver Privacy White Paper(2015), 84

133) 인하대학교 산학협력단, “개인정보 수집 등에 따른 동의절차 방법 개선 및 개인정보보호 관리등급제 도입에 관한 연구”, 방송통신위원회(2014), 165.

만을 통해 위와 같은 차등화된 동의제도의 운영을 이끌어 내기는 어렵다. 현행 법상으로는 우선 동의가 필요한 개인정보와 동의가 필요 없는 정보의 경계를 명확히 구분하는 것이 선행함으로써, 의미 없는 절차와 나열을 가능한 한 생략하여 절차 구성 및 법위반 리스크에 관한 사업자의 부담 및 이용자의 피로도를 줄일 필요가 있다.

관련하여, 결합되지 않은 상태의 개인식별가능정보만을 별도로 취득하여 이를 이용하는 경우 그에 대해 별도의 동의가 필요하다고 보기 어려우며, 이러한 정보에 대해 동의를 요구하는 것은 현실적으로 이행이 불가능하다고 보인다. 예를 들어, 어떤 검색 서비스에 가입한 동일한 이용자가 로그인을 하지 않은 상태에서 검색어를 입력한 경우, 이에 대해 로그인하지 않은 이용자들이 검색어를 입력할 때마다 사업자에게 미리 법적고지사항을 알리고 개인정보 수집·이용에 대한 동의를 받을 것을 요구하는 것은 이용자에게 과도한 불편을 초래하여 사업자의 서비스 유지에 어려움을 발생시키게 될 것이며, 나아가 사업자로서는 개인을 식별할 수 있는 정보를 별도로 결합하지 않는 이상 해당 정보를 통해 개인을 식별할 수 없으므로, 사업자가 이러한 결합을 예정하고 있는 경우가 아닌 이상 이용자의 개인정보 자기결정권 보장의 필요성이 발생한다고 보기도 어렵다. 이미 개인식별정보를 보유하고 있는 사업자는 해당 이용자의 개인정보 및 개인정보 처리 동의를 유효적법하게 얻은 상태에서 부가적인 주변 정보를 추가 수집하는 것에 지나지 않는다. 또한 개인식별정보도 보유하고 있지 않은 사업자라면 누구인지 알 수 없는 이용자에 관한 파편적인 정보를 수집하게 되는 것인데, 별도로 이를 축적하여 특정 개인을 식별하고자 하는 주관적 목적 내지는 의도가 인정되는 경우가 아닌 이상, 개인정보에 해당하지 않는 정보 수집에 대하여 개인정보로서의 처리 동의를 요구할 근거가 없다고 보인다.

다. 개인정보 유출에 대한 대응의무

현행법상 개인정보가 유출될 경우, 해당 정보를 보유하고 있던 사업자는 이

용자에게 유출 사실을 통지하여야 하며, 행정안전부 방송통신위원회 금융감독원 한국인터넷진흥원 등 유관기관에 신고하여야 하며, 그 밖에 피해 최소화 및 재발 방지를 위한 대책 수립 등의 의무를 부담한다. 특히 근래에 들어 개인정보의 유출은 대량의 고의 유출 또는 해킹 사고 등 정형화된 유형 이외에 각종 전산 오류가 발단이 되어 발생하는 경우가 많아지면서, 기존의 유출사고에서 주로 문제된 개인정보가 성명, 주민등록번호, 전화번호, 카드번호 등 비교적 개인 식별성이 높은 정보였던 것에 비하여 개인에 관하여 더욱 더 다양한 정보가 새어나가고 있다.

개인정보 유출 시에 신고 및 통지의무 등을 두는 것은 개인정보는 한번 유출되면 다시 제2, 제3의 피해로 전이될 가능성이 크므로, 개인정보 유출로 인한 피해를 사전에 방지하고 피해자들이 적절히 대응할 수 있도록 하기 위함이다. 따라서 특정한 정보가 유출되었을 때 위와 같은 조치를 하여야 하는지는 해당 정보가 익명의 제3자에 의해 지득되고 사용될 경우 해당 정보주체에게 피해가 발생할 수 있는가가 기준이 되어야 한다. 이에 비추어 볼 때, 개인정보의 사용목적에 따라 달리 취급할 근거는 없을 것으로 생각된다. 한편 또한 수집 출처에 따른 분류 중 공개된 개인정보의 경우, 이미 공개된 것의 경우에는 이를 유출로 볼 수 있는지 의문일 뿐 아니라, 나아가 유출로 본다고 하더라도 사업자의 유출에 의해 피해가 발생한다거나 개인정보 자기결정권이 상실되었다고 볼 수 없으므로 유출에 따른 통지 및 신고 대상에서는 제외됨이 타당하다. 앞서 소개한 2014다235080 판결이 공개된 개인정보에 대해 개인정보자기결정권의 보호가 일부 축소되는 것은 어디까지나 최초 공개의 목적범위가 유지되는 것을 전제로 하고 있다고 하나, 제3자가 이러한 목적범위를 벗어나 위법한 방식으로 이용할 가능성이 존재한다는 점은 유출 전후로 차이가 없기 때문이다.

한편, 식별가능성의 경우 달리 볼 수 있다. 결합되지 않은 상태의 개인식별가능정보의 경우, 그 상태 그대로 유출되었을 때 제3자는 원칙적으로 유출된 정보만을 보아서는 누구에 관한 정보인지 알아볼 수 없다. 예컨대 포털 서비스가

보관하고 있는 이용자의 검색기록이 외부에 노출된 경우를 가정하면, 검색기록이 해당 정보주체를 식별할 수 있는 다른 정보와 함께 유출되지 않은 경우라면 이용자에게 어떠한 피해도 발생했다고 보기 어렵다. 앞서 언급한 것처럼 개인정보의 개념 요소 중 결합의 용이성에 대한 판단은 전지적 관점에서 내려지는 것이 아니라 개인정보 처리의 목적과 의도 등 제반 사정을 함께 고려하여야 하는 것이다. 이에 비추어 볼 때, 결합되지 않은 상태의 개인식별가능정보가 사업자의 의도와 무관하게 통제 범위를 벗어나게 된 경우, 유출된 개인정보를 접한 제3자는 해당 정보를 이용자의 개인식별정보와 결합해내어 특정인을 알아볼 수 없으므로, 원칙적으로 유출에 대해 대응할 법상의 의무도 부담하지 않는 것으로 해석함이 옳다.

그러나 유출의 경우 그 자체로 사후적 조치로서의 성격을 가지고 있기 때문에, 위와 같이 이론상의 분류에 따라 일의적으로 대상 범위에서 배제하기는 어려운 측면이 있다. 예를 들어 다른 일체의 정보 없이 이용자의 이메일주소 또는 아이디 정보만이 유출되었다고 볼 때, 과연 해당 정보들이 결합되지 않은 개인식별가능정보에 불과하다고 하여 이용자에게 어떠한 피해도 발생하지 않은 것으로 볼 수 있는지는 의문이다. 이메일주소나 아이디가 마치 오프라인에서의 성명, 주민등록번호와 같이 온라인상의 정체성의 핵심을 이루는 오늘날 이메일주소만 외부로 노출되었다고 하여 아무런 위험이 발생하지 않는다고 장담하기는 어렵다. 누군가는 해당 이메일 주소를 수집하여 대량 스팸메일을 전송할 수 있고, 또 누군가는 이메일 주소만으로 SNS나 검색엔진 등을 이용하여 해당 정보주체가 누군지까지 찾아낼 수도 있다. 또한 앞서 본 연구서 45면에서 소개한 2017노7275 판결이 결합되지 않은 상태의 개인식별가능정보가 유출된 전형적인 사례라고 할 수 있는데, 해당 사안에서는 법원이 제반 사정을 고려하여 유출된 개인정보를 수령한 자가 당해 정보만으로는 개인을 식별할 수 없다고 판단하였지만, 유출 사고의 내용 및 당사자간의 관계를 고려할 때 결합의 용이성과 식별가능성이 충분히 인정될 가능성이 있다.

이러한 점을 고려할 때, 결합되지 않은 상태의 개인식별가능정보만이 유출된 경우에는 우선 그 자체로 개인정보에 해당하지 않는다는 전제에서 출발하여 피해자인 정보주체가 유출 정보를 접한 타인에 의하여 종국적으로 식별될 가능성이 있는지, 그리고 유출된 정보만으로도 오용 혹은 남용될 가능성이 있는지를 검토하여 예외적으로 그러한 가능성이 인정되는 경우에 한해 유출에 따른 대응 의무가 발생한다고 해석함이 타당하다.

사업자의 관점에서는 유출된 정보가 개인정보에 해당하는지에 관한 판단도 모호한 상황에서 이용자에게 개인정보 유출에 관한 통지를 하고 관련 신고를 함으로써 스스로의 신뢰도를 낮추는 것이 상당한 부담으로 작용할 수 있다. 또한 결합되지 않은 상태의 개인식별가능정보가 유출된 경우에는 피해를 입은 이용자를 특정하기 어려운 경우가 많은데, 그 경우 인터넷 홈페이지에 30일 이상 유출 사실을 게시하여야 하여[134] 사업자의 부담은 더욱 커진다. 이러한 사정을 고려하면, 결합되지 않은 상태의 개인식별가능정보만이 유출된 경우 일률적으로 유출에 따른 대응 의무가 발생한다고 해석하는 것은 사업자의 영업의 자유를 지나치게 제한하는 것으로 보인다. 관련하여, EU의 GDPR은 가명처리된 개인정보를 개인정보 침해(breach) 통지의 범위에서 제외하고 있다는 점도 참고할 수 있을 것이다.

<표 4-5> 개인정보침해 통지에 관한 GDPR 제34조 제3항[135]

3. 다음 각 호의 하나에 해당하는 경우, 제1항의 개인정보주체에 대한 통지는 요구되지않는다. (a) 개인정보처리자가 적절한 기술 및 관리적 보호조치를 시행하였고, 그 조치, 특히 암호처리 등 관련 개인정보를 열람 권한이 없는 개인에게 이해될 수 없도록 만드는 조치가 침해로 영향을 받은 개인정보에 적용된 경우

134) 정보통신망법 시행령 제14조의2 제3항
135) 개인정보보호위원회 번역문

(b) 개인정보처리자가 제1항에 규정된 개인정보주체의 권리와 자유에 대한 중대한 위험을 더 이상 실현될 가능성이 없도록 만드는 후속 조치를 취한 경우
(c) 필요 이상의 노력이 수반될 수 있는 경우. 이 경우, 공개 또는 유사한 조치를 통해 개인정보주체가 동등하게 효과적인 방식으로 통지받도록 해야 한다.

라. 파기의무

개인정보를 보유하는 사업자는 개인정보의 수집 및 이용 목적이 달성되거나, 동의를 얻은 보유기간이 경과한 경우에는 해당 개인정보를 파기할 의무를 부담한다.[136] 앞서 언급한 것처럼, 파기의무를 부과하는 논리적 근거는 사업자가 개인정보를 계속 누적해가며 보유할 경우 그만큼 개인정보 유출 또는 오남용으로 피해가 발생할 가능성이 커진다는 추상적인 위험이다. 단순한 가능성 또는 위험에 근거하여 사업자의 영업자산에도 해당할 수 있는 보유 개인정보를 일괄적으로 파기하도록 하면서 미이행에 대해 형사처벌의 위험까지 부담시키는 것은 지나치게 개인정보의 보호에만 치우친 것으로서, 해석을 통하여 적절히 균형을 회복할 필요가 있다.

파기의무의 근거가 유출의 위험 내지는 동의에 의한 이용범위의 제한인 이상, 앞서 유출에 대한 대응의무 및 동의획득의무의 범위에서 제외되는 것으로 판단한 결합되지 않은 상태의 개인식별가능정보는 파기 대상에서도 제외하는 것이 타당할 것으로 보인다. 이와 같은 정보가 추후 보호조치의무 위반이나 개인정보의 유출로 인하여 개인식별정보와 함께 제3자의 수중에 들어감으로써 이용자에게 어떠한 피해가 발생한다고 하더라도, 이는 각각의 의무 미이행에 따른 결과이지 결합되지 않은 상태의 개인식별가능정보를 파기하지 않은 행위와는 직접적인 인과관계에 있지 않다. 즉 파기가 필요한지 여부는 현재 정보가 보관되어 있는 상태만을 기준으로 판단하는 것이 타당하며, 이에 따르면, 결합

136) 정보통신망법 제29조 제1항 각호

되어 있지 않은 상태의 개인식별가능정보는 제외함이 옳다.

관련하여 최근 방통위가 발간한 온라인 개인정보 처리 가이드라인에서도 유사한 입장을 취한 것으로 이해된다. 동 가이드라인에서 방통위는 개인정보의 파기의무와 관련하여 "회원 DB와 분리된 나머지 DB(거래기록 DB 등)에는 그 자체로 식별가능한 개인정보가 존재하지 않는다면(난수화된 고객번호, ID의 해쉬값 등만 존재하는 경우), 회원 DB 내의 개인정보에 대해서만 파기 또는 분리 저장 관리하는 것도 가능"하다는 입장을 표명하였는데,[137] 규제 적용에 있어서 개인정보의 보관 상태를 적극적으로 고려하여 대상 범위를 합리화한 바람직한 해석례로 생각된다.

반면 사업자가 내부적으로만 사용하는 생성정보의 경우는 특별히 그 사정만으로는 다른 개인정보와 달리 취급하기 어렵다. 개인식별정보와 결합된 상태의 정보를 전제로 하는 이상 문리해석으로는 파기 대상에서 제외할 근거가 없을뿐더러, 동의의 대상으로서 일정한 보유기간 및 보유목적을 알리고 동의를 얻은 것이므로 그 동의의 범위에 구속된다는 문제도 있기 때문이다. 따라서 사업자가 해당 정보를 상태 그대로 보유하며 이용하기는 어려우나, 앞서 언급한 것과 같은 비식별조치를 활용하고, 법 집행기관 역시 개인정보의 비식별화조치를 통한 정보 활용이 활성화될 수 있도록 적극적으로 장려함으로써 정보 보관과 활용에 관한 사업자의 정당한 이익을 존중할 수 있을 것으로 생각된다.

4. IP 주소 및 쿠키 정보에 대한 취급

온라인 환경에서 자동으로 수집되는 정보들은 통상적으로 명백한 개인식별정보를 포함하지 않는 경우가 많아, 그 자체로서 정보통신망법상 각 의무 이행의 대상이 되는지가 논란의 대상이 될 때가 많다. 특히 사업자가 자동수집정보를 개인식별정보 등과 결합하여 사용할 의도가 없고 식별이 불가능한 상태에서의

137) 방송통신위원회, 온라인 개인정보 처리 가이드라인(2018), 19.

전체 데이터셋을 보유 및 분석하는 것만으로도 충분한 이용가치가 있는 경우에, 해당 정보들을 개인정보로서 보호해야 하는가에 대해 사업자와 이용자 간에 이해 갈등이 발생한다. 이와 같은 정보로는 검색기록, 로그기록, 광고 ID, RFID 등 다양한 것이 있으나, 개인정보로서의 보호 범위에 주안점을 두는 본 연구서에서는 상대적으로 개인정보 보호 관점에서 많은 논의가 이루어지고 있는 IP 주소와 쿠키를 대표적인 예시로서 다루도록 한다.

가. IP 주소와 쿠키의 개인정보성

IP 주소, 쿠키, 검색기록 등의 정보는 전통적인 시각에서는 개인에 관한 정보에는 해당하지 않을 수 있다. IP 주소[138]는 사람이 아닌 특정한 기계에 할당된 정보이고, 쿠키[139]는 이용자에게 서비스를 제공하기 위한 기술에 불과하며, 검색기록의 경우 개인의 특징을 포함하거나 추론할 수는 있지만 그 자체로서 특정인과의 고유의 연결성을 갖거나 해당 인물을 설명·묘사하는 정보도 아니다. 인터넷의 보급 및 확산과 함께 개인정보 침해 여부가 문제되었던 이와 같은 정보들은, 특히 새로운 온라인 환경에서 광고 및 마케팅의 핵심 수단으로서 개인에 관한 정보를 무수히 집합하고 이를 근거로 해당 인물의 총체적인 상을 창조하고, 동시에 특정인을 추적하는 실마리로 활용되면서 그 중요성이 높아졌다.

보다 구체적으로는, 쿠키에 저장된 이용자의 활동 기록들(이하에서 “쿠키”라 함은 쿠키에 저장된 활동 기록을 의미함)은 웹사이트 사용을 최적화하기 위해 이용자의 ID와 패스워드, 이전 검색기록 등을 쉽게 불러오기 위해 사용되거나, 나아가 이용자가 관심을 보인 콘텐츠 내역 등 행태정보를 이용한 맞춤형 광고를 위한 목적으로도 활용된다. 온라인상에서의 대표적인 이용자 식별 정보

138) TCP/IP 프로토콜을 사용하여 통신을 할 때, 송신자와 수신자를 구별하기 위한 고유의 주소 (두산백과)

139) 웹사이트에 접속할 때 자동적으로 만들어지는 임시 파일로 이용자가 본 내용, 상품 구매 내역, 신용카드 번호, 아이디(ID), 비밀번호, IP 주소 등의 정보를 담고 있는 일종의 정보파일 (시사상식사전)

인 IP 주소도 마찬가지로 이용자를 추적하여 맞춤형 광고를 하는 데에 이용되고 있다. 헌법재판소가 언급한 "개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경[140]"이 이와 같은 정보의 활용을 통해 실현되고 있는 것이다.

이와 같이 IP 주소와 쿠키는 서로 작동 원리나 목적은 다르지만, 온라인 환경에서 특정인을 알아보기 위한 동일한 식별자 기능을 한다. 특히 IP 주소에 대하여서는 이전부터 개인정보성이 계속하여 논의되어 이미 임시로할당되는 유동 IP마저도 개인정보에 해당한다는 유럽최고재판소 판결[141]이 있었으며, 2018년 5월부터 시행된 GDPR은 개인정보의 정의에 "online identifier"를 포함하면서 그 예시로서 IP 주소, 쿠키를 직접 언급하기에 이르렀다. 미국의 경우에도 마찬가지로, 어린이 온라인 프라이버시보호법(Children's Online Privacy Protection Act 등에서 IP 주소와 쿠키를 개인정보에 해당하는 것으로 명시하고 있다.

<표 4-6> GDPR 상 온라인 식별자 관련 규정[142]

제4조 정의 본 규정의 취지에 따르면 (1) 개인정보는 식별된 또는 식별 가능한 자연인('개인정보주체')과 관련한 일체의 정보를 가리킨다. 식별가능한 자연인은 직접 또는 간접적으로, 특히 이름, 식별번호, 위치정보, **온라인 식별자**를 참조하거나 해당인의 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특이한 하나 이상의 요인을 참조함으로써 식별될 수 있는 자를 가리킨다. 전문 (30) 개인은 본인이 사용하는 기기, 애플리케이션, 툴, 프로토콜을 통해 제공되는 **인터넷 프로토콜 주소, 쿠키 식별자** 또는 전파식별태그 등의 기타 식별자인

140) 헌법재판소 2005. 7. 21. 선고 2003헌마282 결정
141) Patrick Breyer v Bundesrepublik Deutschland, C-82/14(2016), ECLI:EU:C:2016:930.
142) 개인정보보호위원회 번역문

온라인 식별자와 연결될 수 있다. 특히 이러한 정보는 개인에 대한 자취를 남겨, 이러한 정보가 서버를 통해 전해지는 독특한 식별인자 및 기타 정보와 결합되는 경우, 해당 개인에 대한 프로파일을 생성하고 이들을 식별하는 데 사용될 수 있다.

<표 4-7> 미국 Children's Online Privacy Protection Act 관련 규정

Personal information means individually identifiable information about an individual collected online, including: (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, **a customer number held in a cookie, an Internet Protocol(IP) address**, a processor or device serial number, or unique device identifier;

우리 정보통신망법에서도 개인정보 처리방침에 포함시켜야 할 사항으로서 "인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항"을 정함으로써[143] 쿠키에 관한 규율을 일부 정하고 있으며, 방통위의 온라인 개인정보 처리 가이드라인은 열람제공요구권 등의 부분에서 IP 주소나 쿠키를 예시로 언급하면서 이들 정보가 개인정보에 해당하는 것을 전제로 하고 있다.

나. 정보통신망법상 IP 주소 및 쿠키에 대한 취급의 문제

IP 주소와 쿠키가 개인정보에 해당할 수 있다면, 앞서 살펴본 정보통신망법상의 각 규제에 대한 해석론 역시 IP 주소와 쿠키에 동일하게 적용될 것이다.

IP 주소는 단독으로 보관된 상태에서는 이용자 개인을 식별할 수 없다. 물론 IP 주소가 범죄 수사 등의 목적으로 온라인상의 게시글 또는 활동내역으로부터 해당 인물을 추적해내기 위해 빈번하게 사용되는 수단이기는 하나, 이는 인터

143) 정보통신망법 제27조의2 제2항 제6호

넷 서비스를 제공하는 통신사가 서버에 남긴 기록을 조합하여야만 가능하며, 이 때 확인되는 것 역시 특정 인물이 아닌 사용된 컴퓨터가 무엇인지에 한한다는 점 등을 고려하면 여러 단계의 추적이 필요한 IP 주소를 개인식별정보라고 보기는 어렵다.

이와 같이 IP 주소는 '결합되어 있지 않은 개인식별가능정보'의 지위에 있지만 동시에 '결합되어 있지 않은 개인식별가능정보'를 개인식별정보와 매칭하는 수단이 된다는 점에서 특징이 있다. 예컨대 로그인하지 않은 이용자의 검색기록 등은 오직 사용자가 파악하고 있는 계정 소지자의 IP 주소 등과 매칭될 경우에만 이용자의 다른 신원 정보와 연결될 수 있다. 만일 사업자가 그와 같은 매칭을 통한 식별 작업을 행할 의도나 계획이 없이, 다른 식별정보와 분리된 상태에서 비실명 이용자들의 이용기록과 IP 주소를 처리하는 경우라면, 해당 정보는 앞서 전개한 해석론상 '결합되어 있지 않은 개인식별가능정보'의 지위에 있다. 이에 따라 볼 때, 이용자의 IP 주소는 개인식별정보와 분리되어 있는 이상 정보통신망법상 열람 제공, 이용내역 통지 및 파기 의무의 대상에서 제외됨이 옳다. 또한 IP 주소만이 외부에 유출된 경우 그로 인한 이용자 식별 및 오남용의 위험성도 생각하기 어렵고 마찬가지로 결합을 전제로 하지 않는 한 개인 식별이 불가능하므로, 사업자는 IP 주소에 대해 유출 대응 의무 및 수집 동의 의무도 부담하지 않는 것으로 보아야 할 것이다.

쿠키의 경우, 정보를 저장하고 불러오는 기술을 지칭하는 것이기 때문에 IP 주소와 달리 그 내용이 단일하지 않다. 이용자가 쿠키가 심겨져 있는 웹사이트에 방문할 경우 쿠키의 설계 목적에 따라 쇼핑 정보, 관심사 등의 행태정보에서부터 나아가서는 지역, 이메일 주소, 신용카드번호, 이름 등 사업자가 수집하고자 하는 매우 다양한 정보가 저장될 수 있다. 물론 해당 정보는 사업자측이 아닌 이용자 컴퓨터의 하드디스크 내에 저장되며, 쿠키의 내용 중 value값은 대부분 암호화되어 있기 때문에 저장된 상태의 정보만으로는 내용을 이해할 수조차 없는 경우가 대부분이다. 그러나 물리적으로 사업자의 영역에 보관되지는

않더라도 이용자의 이용 기록 내지는 활동 기록을 읽어내고, 필요 시에 불러내어 확인할 수 있도록 설계된 것이므로 사업자가 수집하여 이용하는 정보라고 볼 수 있다.

이와 같이 쿠키에는 개인식별정보와 개인식별가능정보가 모두 포함되어 있을 수 있다. 이 중 개인식별가능정보로서 개인식별정보와 결합되어 있지 않은 것은 앞서 IP 주소와 동일한 결론이 적용된다. 쿠키가 암호화 없이 평문으로 전송 또는 저장되어 있는 경우, 사업자가 쿠키를 탈취하여 사용하는 공격자를 정당한 이용자로 인식하여 각종 개인정보를 노출하게 될 수 있으므로 보호조치가 필요하다. 그러나 쿠키가 개인식별정보와는 결합되지 않은 상태에서 쿠키만이 유출되는 경우에는 일반적으로 그에 따른 오남용의 위험이 있다고 보기 어려워 유출에 따른 통지 및 신고 의무가 발생한다고 보기 어렵다. 다만 이메일 주소나 전화번호와 같이, 유출되는 경우 그 자체로서 오남용의 위험이 있는 정보가 포함된 경우에는 별도로 개인식별정보와 결합되지 않은 상태라고 하더라도 예외적으로 유출에 따른 대응 의무가 요구된다고 볼 수 있으므로, 어떤 정보가 저장된 쿠키가 유출되었는지에 따른 개별적인 판단이 필요하다고 보인다.

또한 쿠키의 내용 자체를 사업자가 상시 보관하며 식별정보와 결합 사용하는 것이 아닌 한, 그 밖에 매 이용기록을 저장할 때마다 동의가 필요하다거나 쿠키 정보의 열람 및 제공에 응할 의무, 이용내역 통지 및 파기 의무가 요구된다고는 보기 어렵다. 단 쿠키에 저장된 개인정보에 대한 것이 아니라 쿠키 자체의 운영 내역 또는 쿠키를 차단 또는 삭제하는 방법에 대하여는 각 정보주체인 이용자에게 알릴 필요가 있으며, 이러한 취지가 실정법에 반영된 것이 “인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항”을 알리도록 하는 정보통신망법 제27조의2 제2항 제6호에 해당하는 것으로 생각된다.

제 5 장 결 론

이상과 같이 개인정보에 관한 규제 유형별로 보호범위를 차등화할 수 있는 해석방안에 대해 살펴보았다. 정보의 활용이 곧 기업과 국가의 경쟁력으로 연결되는 오늘날, 개인정보의 개념이 추상적이고 모호하다는 등 개념정의상의 문제점에 천착하여서는 안 될 것으로 생각된다. 그와 같은 문제의식을 명확히 갖고, 개인정보 관련 법령상의 각종 규제를 합리화함으로써 보호와 이용을 동시에 꾀할 수 있는 적극적인 해석 방안을 마련하는 것이 필요하다.

본 연구서에서는 그 출발점으로서 정보통신망법상의 규제를 보호조치의무, 동의획득의무, 유출에 대한 대응의무, 파기의무, 열람제공요구에 대한 조치의무, 이용내역의 통지의무로 단순화한 후, 사업자와 이용자 사이의 합당한 이익형량에 따른 해석 방안을 도출하고자 하였다.

특히 개인정보 관련 법령의 해석에 있어서 개인정보의 보호 측면이 지나치게 강조됨으로써, 그로 인해 제한을 받는 사업자의 창의, 영업비밀, 영업의 자유 등은 상대적으로 경시되고 있는 것은 물론, 현실적인 법 적용 및 준수 가능성마저 확보하기 어려운 해석이 일부 제시되고 있다는 점에 주목하여 보다 합리적인 방안을 제시하고자 노력하였다.

이번 연구와 같이 개인정보 관련 규제의 적용 범위를 합리화하려는 시도가 축적됨으로써 입법과 정부의 해석에 반영되어, 서비스 제공자와 이용자 양측의 권리가 합당하게 수호되고 사회 전체의 비용 내지 불편이 줄어들 뿐 아니라, 향후 ICT 신산업 시대에 걸맞는 규제환경을 갖출 수 있게 될 것을 기대한다.

참 고 문 헌

국내 문헌

(단행본)

개인정보분쟁조정위원회, 2013년 개인정보분쟁조정사례집(2013)

국무조정실·행정안전부·방송통신위원회·금융위원회·과학기술정보통신부·
보건복지부, 개인정보 비식별 조치 가이드라인(2016)

김대휘·김신 편집대표, 주석 형법(각칙 2)(제5판), 한국사법행정학회(2017)

김상용, 채권각론(제2판), 화산미디어(2014), 393

김성돈, 형법각론(제4판), 성균관대학교 출판부(2016)

김용담 편집대표, 주석 민법 총칙(3)(제4판), 한국사법행정학회(2010)

김형배, 채권각론(제2판), 박영사(2001), 577

방송통신위원회, 온라인 개인정보 처리 가이드라인(2011)

_____, 온라인 개인정보 처리 가이드라인(2018)

배종대, 형법각론(제8판), 홍문사(2013)

오영근, 형법각론(제3판), 박영사(2014)

이재상 외 2인, 형법각론(제10판), 박영사(2016)

이창범, 개인정보 보호법, 법문사(2012)

한국CPO포럼, 개인정보 관련 제재 및 피해구제 합리화 방안 연구(2013)

한국인터넷법학회, 개인정보 보호와 적정 활용의 조화를 위한 제도 도입 연구
(2009)

한국인터넷진흥원, 2012. 8. 개정 정보통신망법 개인정보보호 신규제도 안내서
(2012)

행정안전부, 개인정보보호 법령 및 지침 고시 해설(2016)

(논문 등)

고유흠, “빅데이터와 개인정보보호”, 이슈와 동향 21권(2014)
고학수・최경진, “개인정보의 비식별화 처리가 개인정보 보호에 미치는 영향에 관한 연구”, 개인정보보호위원회(2015. 4)
권순희, “전통적 법해석방법과 법률해석의 한계”, 가톨릭대학교 법학연구소 법학연구(2009)
권영준, “개인정보 자기결정권과 동의 제도에 관한 고찰”, 2015 Naver Privacy White Paper(2015)
김경환, “규제 측면에서의 한국 EU 일본의 개인정보 보호 법령의 비교”, 2017 Naver Privacy White Paper(2017)
김웅규, “위헌심사기준으로서의 명확성과 광범성무효의 원칙”, 공법연구 제35집 제3호(2007)
김일환, “개인정보의 보호와 이용법제의 분석을 위한 헌법상 고찰”, 헌법학연구 제17권 제2호(2011)
김정섭, “주민등록번호 없는 ‘클린 인터넷’ 환경 조성”, 통신연합 제61호(2012), 23.
김학태, “법률해석의 한계 - 판례에서 나타난 법해석방법론에 대한 비판적 고찰”, 외법논집 제22집(2006)
김현경, “개인정보보호제도의 본질과 보호이익의 재검토”, 성균관법학 제26권 제4호(2014)
박광배 외 2인, “빅데이터 시대 생성정보의 처리 체계”, 정보법학(2017)
박민우, “개인정보 보호법상 불확정 개념에 있어 형법의 보장적 기능을 확인해주는 해석과 사회상규의 역할”, 형사정책연구 제28권 제1호(2017)
심헌섭, “법철학적 법학방법론 - 법철학과 합리적 법학방법”, 서울대학교 법학 제24권 제1호(2003)
윤진수, “허위표시와 제3자”, 민사판례연구 제29권(2007)
이경호, “정보화사회에 있어서 프라이버시권의 보호: 개인정보처리에 관한 프

라이버시권의 법적 보호를 중심으로", 박사학위논문, 동국대학교(1986)
이대희, "프로그램 포맷의 법적 위상과 보호방안에 관한 연구", 고려법학 제79호(2015)
이인호, "「개인정보 보호법」상의 '개인정보' 개념에 대한 해석론", 정보법학 제19권 제1호(2015)
이준구, "개인정보의 보호", 법학논거(1991)
이희옥, "개인정보 자기결정권에 관한 비판적 검토", 법제 통권 제675호(2016)
인하대학교 산학협력단, "개인정보 수집 등에 따른 동의절차 방법 개선 및 개인정보보호 관리등급제 도입에 관한 연구", 방송통신위원회(2014)
인하대학교 산학협력단(법학연구소), "개인정보의 범위에 관한 연구", 개인정보보호위원회(2014)
조성은, "개인정보보호 법제 하에서의 정보 활용성 향상 전략", KISDI Premium Report 제17권 제12호(2017)
채성희, "개인정보자기결정권과 잊혀진 헌법재판소 결정들을 위한 변명", 정보법학 제20권 제3호(2016)
최호준·안황권, "개인정보보호에 관한 연구", 경기행정논집(1991)
황성기, "개인정보 보호와 다른 헌법적 가치의 조화", 경제규제와 법 제5권 제2호(2012)
황우여, "개인정보보호법. 정보공개법(시안)", 고시계(1989)

(기타)
인재근 의원 대표발의, "개인정보 보호법 일부개정법률안", 2016621, (2018. 11. 15.) [계류중], 5(제2조 제1호)
김일환, "온주 개인정보보호법", 온주,
http://www.onju.com/onju/service/writer/edit/SER_WEB03_1.aspx?lawid=243&lawtitle=%uAC1C%uC778%uC815%uBCF4%uBCF4%uD638%uBC95&commentid=0&l

awnbId=00695240&decl=%uC81C1%uC870&state=0#76941|1|%uC81C2%uC870|3 (2018. 11. 1. 최종 확인)

해외 문헌

(단행본)

Bird & Bird, Data Ownership - Building the European Data Economy(2017)

The Article Working Party, Opinion 4/2007 on the Concept of Personal Data (2007)

_____, Opinion 5/2014 on Anonymization Techniques(2014)

Thomas Cooley, Law of Torts(2nd ed.), Chicago: Callaghan & Co. (1888)

Yolande Berbers et al., Privacy in an Age of the Internet, Social Networks and Big Data, Royal Flemish Academy of Belgium for Science and the Arts (2018)

(논문 등)

Charles Fried, "Privacy", 77 Yale Law Journal 475, 482 (1968)

Elisa Bertino & Elena Ferrari, “Big Data Security and Privacy”, 31 Studies in Big Data (2017)

European Data Protection Supervisor, “Meeting the challenges of big data”, Opinion 7/2015 (2015)

(기타)

日本 個人情報保護委員会, 個人情報の保護に関する法律ついてガイドラン(通則編)(2017. 3.)

_____, 「個人情報の保護に関する法律についてのガイドラ

イン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ(2017)
日本　総務省，電気通信事業における個人情報保護に関するガイドライン(2017.9.)

저 자 소 개

이 성 엽

- 고려대 법학과 졸업
- 서울대 행정대학원 행정학 석사
- 미네소타대학교 법학과 석사
- 서울대 법학과 박사
- 현 고려대학교 기술경영전문대학원 초빙교수
- 현 한국미래법정책연구소 대표

권 영 준

- 서울대 법학과 졸업
- 서울대 법학대학원 법학 석사
- 하버드대학교 로스쿨 법학 석사
- 서울대 법학대학원 법학 박사
- 현 서울대 법학전문대학원 교수

방통융합정책연구 KCC-2018-45

개인정보 보호 범위 차등화에 관한 연구

2018년 12월 30일 인쇄
2018년 12월 30일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
경기도 과천시 관문로 47
정부과천청사
TEL: 02-2110-1323
Homepage: www.kcc.go.kr